# Baltics Aff

# Notes

Shout out to Kevin Lai, Archan Sen, Lily Ren, Daniel Gallagher, and Brandon Yao for their work on this file.

The aff would have the US work to cooperate with NATO Baltic States on cyber defense. It would be a form of mutual cooperation where the US would help provide information and expertise towards Baltic States and states such as Estonia would share information regarding combating Russian cyber disinformation campaigns, attacks, etc.

# Potential 1ac

## Cyber Advantage

#### Ukraine set the brink – Russia will put pressure on NATO via cyber threats on the Baltic

Cerulus 2-22 (Laurens Cerulus leads POLITICO Europe’s team of reporters covering cybersecurity, privacy and data protection issues as Cybersecurity Editor. He also supports the broader team of reporters covering technology issues as Deputy Technology Editor. He is a graduate of City University London’s journalism department and holds master’s degrees in history and international politics. He is a Belgian, born in Leuven. “Cyber ‘spillover’ from Ukraine looms in the Baltics” <https://www.politico.eu/article/baltic-cyber-spillover-ukraine-russia-attack/)LR>

The conflict between Russia and Ukraine puts neighboring EU countries at risk of disruption from cyberattacks and the spread of disinformation, officials warned Tuesday. "The Baltic states, for Russia, are the easiest way to put pressure on the EU and NATO ... This is the place where **we have to pay careful attention**," said Bart Groothuis, Liberal member of the European Parliament and former cybersecurity official at the Dutch Ministry of Defense. Groothuis is leading a delegation of members of the European Parliament's subcommittee on defense and security on visits to Estonia on Tuesday and Lithuania on Wednesday, in what he said was a "show of solidarity" with Ukraine. Those two Baltic countries are already involved in a cyber defense operation to support Ukraine through the EU's Cyber Rapid Response Team, which was activated Tuesday. The threat of cyberattacks on European soil is two-fold: First, attacks launched on Ukrainian networks could spread to European networks. Second, Russia could choose to launch direct attacks on European targets through its intelligence services or cybercriminal groups to disrupt the West's response to the Ukraine crisis. Cyberattacks on Ukraine have affected Europe in the past. In 2017, hackers spread malware known as NotPetya through a Ukrainian piece of software and triggered a worldwide cyber crisis seen as the most devastating cyberattack in history. Western security services later attributed the attack to Russia's military intelligence agency GRU. "There is always the threat of a spillover" like NotPetya, said Jaak Tarien, director at the Cooperative Cyber Defence Centre of Excellence (CCDCOE), a NATO-accredited cyber defense center based in Tallinn that advises the defense alliance and its members on cybersecurity. "It's the one internet we're using," Tarien said, pointing to the connections Europe's tech networks have with Ukraine. Baltic countries, in particular, in past years were often the target of campaigns by Russian state-backed hacking groups targeting public and private institutions. The EU attributed a campaign known as "Ghostwriter" at least in part to Russia, after it first plagued Baltic countries with phishing emails and disinformation campaigns and then moved on to target Polish and German politicians. Countries like Estonia and Lithuania have also emerged as vocal proponents of a tougher response to Russian cyber aggression in Europe. Officials in the Baltics are now on high alert, expecting more attacks to come from Russia as the conflict in Ukraine escalates. Last week, Lithuania's Ministry of Defense raised the alarm, saying it expected serious cyberattacks on the country's public authorities. "We definitely see how, as the general state of security deteriorates, the likelihood of cyber activities increases. We're working on a higher alert level," said Margiris Abukevičius, vice minister at the Ministry of National Defense in Lithuania.

#### Russia will use disinformation in order to destabilize the region

Horchakova 2022, Veronika Horchakova Mykolas Romeris University, European and International Business Law program, Master’s degree student (“STRENGTHENING THE TRANSATLANTIC PARTNERSHIP: CHALLENGES AND OPPORTUNITIES FOR THE BALTIC STATES” https://repository.mruni.eu/bitstream/handle/007/18311/Teisines\_minties\_svente-97-107.pdf?sequence=1)

The other non-military threat for the Baltic region is Moscow’s use of the Russophone minority as political instruments against the West. For example, signs of warfare were identified when Russian-speaking inhabitants in Vilnius received brochures with disinformation on the economic situation in Lithuania and a call to participate in the resettlement of ethnic Russians from Lithuania to Russia.13 This kind of propaganda was also used in Ukraine to disrupt loyalty to the State. The Baltic countries need to create a “defensive shield” to fight against Russia’s disinformation and propaganda. Moscow’s primary goal is to form a positive opinion of Russia among local inhabitants by creating dissatisfaction with the relevant governments, shaping and misrepresenting historical facts, and exploiting the vulnerabilities of the Baltic’s political systems, economy, and society. Here the Lithuanian case can serve as a guide for the other two Baltic States and NATO members, too. The roots of the anti-Russian propaganda and disinformation campaign originated in 2016, when Lithuania introduced temporary bans on Russian media outlets that breached pre-existing media laws.14 Shortly after that, the Lithuanian parliament adopted an ordinance restricting Russian media production content on Lithuanian TV. In 2018, the Lithuanian parliament adopted new amendments to the Public Information Law. TV channels in Lithuania must translate TV programs into Lithuanian “if these programs are produced in Russian or other non-EU languages and broadcast for longer than one hour and a half.”15 Such restrictions are effective at diminishing the Russian influence, but are not a panacea. As for cyber security, the Baltic States have undertaken successful work in combating cyber-attacks. According to the International Telecommunication Union’s Global Cybersecurity Index 2020, among 194 countries, Estonia is ranked third after the US and the UK. Followed by the Russian Federation, Lithuania is the sixth-best cyber protected country. Latvia completes the list of the top 15.16 This ranking is based on five pillars: legal, technical, organizational, capacity building, and cooperation measurements related to cybersecurity. Since 2019, these countries have each had Cyber Security Strategies, but we have to consider that these rankings are not always reliable, and sometimes they do not represent reality in all its shapes. Despite establishing the NATO cooperative Cyber Defence Centre of Excellence in 2008 (hosted by Estonia), several commentators have criticized the real cyber warfare capabilities of NATO. In a 2019 interview, the former supreme allied commander of NATO, Adm. James Stavridis, USN (Ret.), warned that “in cyber, and cybersecurity, we have the greatest mismatch between the level of threat and level of preparation.”17 New asymmetric or technological threats require extensive cooperation not only within but also outside of the Alliance. The security and defence sectors in the Baltic States need to build partnerships with the private and academic sectors, all of which will need to cooperate with each other to maintain situational and technological awareness.18 It is clear that, in reality, the ongoing conflict between western countries and Russia does not take place inside tanks or submarines but behind a computer. Russia has massively increased its cyber warfare capabilities and is particularly strong in social manipulation and other cyber-attacks. In this context, there are signs of significant commitment over time to enable the Baltic countries to develop their national defence further. For example, the Baltic States have already signed a five-year roadmap of defence cooperation with the Pentagon,19 meaning that, by 2024, capability development and defence-related aid, training exercises, and cyber defence will be exercised with the US. Officials emphasized the benefits of this program and said that they look forward to its further development. Activated transatlantic relationships are the perfect opportunity for Lithuania, Latvia, and Estonia to generate new partnership programs, agreements, and projects against Russian soft power.

#### Aims to destabilize Baltics separate from NATO makes deterring Russia impossible – now is key after Ukraine

Kols 2022, Rihards Kols Chairman of the Foreign Affairs Committee The Saeima (Parliament) of the Republic of Latvia (3/17/2022 “Hybrid Threats: The Baltic Perspective” https://www.csce.gov/sites/helsinkicommission.house.gov/files/RKols\_Hybrid%20threats%20Baltic%20Perspective-2022.pdf

Since regaining our independence from the Soviet Union in 1990, Latvia, Lithuania, and Estonia have been under constant Russian pressure. This pressure has manifested itself is through the conventional military threat, punctuated by ongoing airspace violations by Russian military aircraft and navy, unannounced, large-scale military exercises of inherently offensive nature along their borders, and the general disposition of Russia's military forces in regions closest to the Baltic borders, doing so under the pretence of counteracting the "hostile West" and promoting militarism. Influence, psychological, and information operations have been part of Russian doctrine since the early days of the Soviet Union, but historically they have been relegated to supporting roles. Nevertheless, as General Gerasimov has observed and thus included in the Russian military doctrine, non-kinetic are exceedingly practical, and these instruments will become dominant in future warfare. This is reflected in most current Russian foreign, security and defence policies and doctrinal documents. For years, the strategic goal of Russian information operations in the Baltic states has been to create distance between the Baltics and the West. The Russian concept is rooted in the idea that democratic societies are vulnerable to political manipulation, and exploiting this perceived weakness is far less costly than pursuing annexation or occupation. Consequently, Russian information operations in the Baltics focus on nine objectives: (1) Encourage and support armed actions by separatist groups to promote chaos and territorial disintegration; (2) Increase polarisation between elites and society to foment a crisis of values followed by process of orientation toward Russian values; (3) Demoralise the military and otherwise attrit resolve; (4) Undermine socioeconomic stability; (5) Engender socio-political crisis; (6) Intensify simultaneous forms and models of psychological warfare to demoralise the Baltic states' armed forces and population and break their resolve; (7) Incite mass panic and degrade confidence in crucial government institutions; (8) Defame political leaders not aligned with Russian interests; (9) and Undermine international alliances and partnerships.12 Russia seeks to achieve its strategic ends in the Baltics through influence operations rather than conventional means. Recognising resistance to deeper ties with Russia in the Baltics, Russia has diversified its messaging beyond pro-Russia content. Instead, the Russian strategy is to attempt to convince members of the population that their countries' current alignment with the West, embrace of democracy, and membership in NATO and the EU are in some way detrimental, degrading or dangerous. Russia heavily leverages Russian and local-language traditional media, social media, and the internet toward this end. There is no universally agreed definition of hybrid threats, considering that a wide range of activities falls under this term. Moreover, hybrid threats evolve constantly, and new means in hybrid warfare emerge. However, the European Centre of Excellence for Countering Hybrid Threats defines hybrid threats as "an action conducted by state or non-state actors, whose goal is to undermine or harm a target by influencing its decision-making at the local, regional, state or institutional level. Such actions are coordinated and synchronised and deliberately target democratic states and institutions' vulnerabilities". 3 The use of hybrid tactics often is based on trying to undermine fundamental democratic values and liberties, and it is done under what some call a "chaos strategy". Russia sows chaos to achieve its agenda beyond its borders by deploying an array of hybrid warfare tools - hybrid warfare is a tactical application of the chaos strategy. Total spectrum warfare deploys a blend of conventional and nonconventional means to affect on the ground changes in target populations or territories while seeking to avoid direct military confrontation. Hybrid warfare is employed in a tailored way to sow chaos in target countries. Such efforts generally include irregular warfare, active measures, and special operations. Like the world, hybrid war is not static, and new tools are developed and employed constantly. For the Baltics, having lived in this environment for the majority of their lives, both under Soviet occupation and after regaining their countries' independence, this multi-vector warfare - hybrid warfare tactics and the chaos they attempt to create, have become intuitively recognisable and often seep into the background like white noise.4 From the perspective of the Baltic states, the development of hybrid threat-related policies at the EU or NATO level has been a natural consequence of the changing security landscape in Europe, especially the gradually deteriorating relations between the West and Russia. In the immediate aftermath of Russia's first attack on Ukraine's sovereignty and territorial integrity, different hybrid attack scenarios against one of the three Baltic states were envisaged, e.g., Russia's attempt to overtake Narva, a city in the extreme eastern point of Estonia, where more than 80% of the population are ethnic Russians; or the so-called "little green men", armed soldiers without insignia that were seen in Crimea in March 2014, entering Latgale, the region in Latvia's east5 ; or Russia creating an incident linked to Kaliningrad – the Russian enclave on the Baltic sea wedged between Lithuania and Poland. In the event of any war between Russia and NATO countries, it is through this gap that NATO would have to rush reinforcements and supplies from Poland to the Baltic countries, and it is this gap that Russia would have to close to prevent that. Military strategists have long suggested that Russian forces from Belarus could attempt to punch across the narrow Lithuanian territory known as the Suwalki Gap to the Moscow-controlled enclave of Kaliningrad, effectively cutting off the three Baltic states. 6 These scenarios included Russia sending troops to "restore order" in case of an uprising in Kaliningrad or sabotaging the train lines across Lithuania that serve as a vital transit corridor from Russia. Because Baltic rail infrastructure is still primarily dominated by Soviet-era rails of a specific gauge width, one incompatible with the EU standard rail gauge width, the risks are substantial enough to cause concern. It has been considered that Russia could use the same pretext as in Ukraine, i.e., protection of the Russian-speaking minorities, to target one of the countries in the region, or rely on state-controlled Russian TV channels widely watched by ethnic Russians in the Baltics to spread propaganda and air true and imagined grievances.7

#### Disinfo wrecks Baltic stability. Prefer the first and only statistical study.

SEM = structural equation modeling method

Morkūnas 7-12 [Mangirdas Morkūnas, Faculty of Economics and Business Administration, Vilnius University; 7-12-2022; "Russian Disinformation in the Baltics: Does it Really Work?"; Taylor & Francis; https://www.tandfonline.com/doi/abs/10.1080/10999922.2022.2092976; KL]

Introduction In recent years, awareness of Russian disinformation activities and disinformation efforts has been growing both in the West and in Central and Eastern Europe (Baumann, 2020; Kuczyńska-Zonik & Tatarenko, 2019). Russian disinformation is considered to have achieved some success even in the most developed western countries, where it is presumed to have interfered in the election campaign in the USA (Golovchenko et al., 2020), harassed and impeded independent investigations in Western Europe (Aro, 2016), sought to impair public support for Western assistance to former Soviet countries (Richey, 2018), and significantly affected the election campaign in France (Makhashvili, 2017). Among the main targets for Russian disinformation are the former Soviet Union countries that in Russia are referred to by a unique term coined in 1992, called “near abroad,” (ближнее зарубежье) which attempts to emphasize their status as foreign countries not fully recognized by Russia (Rotaru, 2018). Russian disinformation in the “near abroad” countries seek two main objectives: to inflict as much damage to the statehood of the target countries and to portray Russia in much better colors in the eyes of their citizens (Shakrai, 2015), typically by distorting historical events (Ehrlich, 2021). Although the aim of preventing former Soviet Union Republics from fully diverging from the Russian sphere of influence (Cooley, 2017; Dunn & Bobick, 2014), the Russian Federation has made the Baltic States a target of continuous negative disinformation and psychological subversion tactics (Veebel, 2015), making the disinformation dominated by negative messaging (Thornton & Karagiannis, 2016). It is even stated that among all the European nations, citizens of the Baltic States experience the most concentrated and sophisticated disinformation efforts as an expression of soft power (Simons, 2015). Such Russian disinformation has been affecting the citizens of the Baltic States for more than the past three decades. Arguably residents of the Baltic States are believed to be more susceptible and receptive to various forms of Russian disinformation, having been subject to some 50 years of Soviet brainwashing (Schuhrke, 2019; Thompson, 2019). Such disinformation increases dissatisfaction with domestic governments (Golovchenko, 2022) and the state of democracy generally (Oates, 2016), lowers incentives for personal self-development (Benkler et al., 2018), and provokes anger and social inequality within society (Bardach-Yalov, 2012). There are additional thoroughly documented cases about the intimidation of Baltic States from the Russian side. Matthews (2020) points out at Russian actions aimed at increasing ethnic tensions within these countries. It becomes possible because Baltic States have a significant Russian minority (Best, 2013). Russia is also fully engaged in spreading false information about the possible revision of various treaties between the Baltic States and Russia (Matthews, 2020) up to revoking the recognition of Lithuanian independence (Labanauskas, 2022). Baltic States also have been a subject of various cyber-attacks from Russian based hackers and are expected to experience even more sophisticated cyber-warfare activities it in a foreseeable future (Mälksoo, 2018). The position of Baltic States as a frontline in a cyber-warfare was acknowledged also by NATO by a decision to establish its cooperative cyber-defense competence centre of excellence in one of the Baltic States – Estonia (Kovács, 2018). In this study the follow the definition of disinformation presented by Bayer et al. (2019). It covers the spreading of information which is designed to be false or manipulated or misleading. It also has the intention of generating insecurity, tearing cohesion or inciting hostility, or directly to disrupt democratic processes (Bayer et al., 2019, p. 18). Although in recent years, Russian disinformation reached the level of “strategic information operations” (Flanagan et al., 2019), there have been very few studies on the actual effect of such disinformation. Completed studies were based on qualitative evaluations (Surowiec, 2017), focused on Western countries (Carter & Carter, 2021), or investigated only specific issues – mostly the Russia-Ukraine dispute (Gerber & Zavisca, 2016). Therefore, the present paper aims to evaluate the effect of Russian disinformation on the Baltic States. In order to assess the latent variables related to the effect of disinformation activities on citizens’ minds, this paper uses the structural equation modeling method (SEM), in which a partial least squares technique is employed. To our knowledge, this is the first study on the effect of disinformation on the target countries’ populations using sophisticated statistical methods. The study consists of several parts: the introductory section provides a brief overview of the aims and impact of Russian disinformation in the Baltics, the “Materials and Methods” section introduces the research model and the hypotheses for the study, and the main results are presented in the “Results” section. Finally, the “Conclusions and Discussion” section summarizes the insights of the study, juxtaposes it with the prevailing theoretical streams, and offers directions for future studies in the subject area. Theoretical background There is increasing debate about the socio-political consequences of negative disinformation. Arguably, disinformation enables the success of populist parties during election campaigns (Chernobrov & Briant, 2020) and affects political decisions, as politicians are reluctant to take actions that are potentially unpopular with certain voting groups (Acemoglu et al., 2013) that could be subject to various disinformation tactics (Van Herpen, 2015). Prolonged negative disinformation campaigns lower public participation (Bonch-Osmolovskaya, 2015) through both increased perception of negligibility of voters actions (Van Herpen, 2015) and increased apathy (Gulenko, 2021). In recent years, the intensity of Russian disinformation has substantially increased, especially on social media (Prier, 2020). One of the main aims of destructive Russian disinformation, which has intensified since 2014, is to discredit national authorities by questioning the independence of their actions or decisions (Lelich, 2014). This leitmotif of the “other hand ruling the government” has also been applied through information warfare against another post-soviet country – Ukraine – and is considered to be highly effective (Karlsen, 2016). It also increases citizens’ perception of hostility with respect to the surrounding environment and diminishes their participation in public life and socio-economic activity (Irisova, 2015). Furthermore, Russian disinformation in post-Soviet states boosts nihilism to substantially undermine the economic activity of their populations, especially with respect to future gains (Julukhidze, 2020). Nihilism as a result of increased distrust provoked by Russian disinformation is mentioned by Paul and Matthews (2019), and Russian disinformation objectives to create and facilitate distrust in Government were also noticed by Sanovich (2017). Disinformation also violates the self-identity and perception of justice (Blouin & Mukand, 2019). Reflections on the exaggerated perception of corruption within the state apparatus were found to be one of the most discussed topics (Miller, 2019). The emphasized narrative of the “failed state” in which everything is decided in advance, and in which citizens can neither influence policy decisions nor be the masters of their own personal or career development, is also important for Russian disinformation architects (Helmus et al., 2018). The disinformation-related influence of diminished motivation for positive, personal development has also been mentioned by Smith and Lasswell (2015). Attempting to undermine the perception of safety within the country through constant intimidation and threat of imminent military actions is another major tactical aspect of Russian disinformation (Giles et al., 2015). Although in the short term, the effect may be opposite to that expected by the disinformation designers – a consolidation of the nation in the face of immediate aggression (Yurkova, 2018), in the long term, it rewards the disinformation creators in the form of decreased trust in public institutions (Haas, 2017) and the state itself (Redley, 2007) in the target country. Such dual effects of disinformation not only increase the complexity of how it may be detected, (Kausar et al., 2020) but also make understanding its effects even more puzzling. It has been noted that although Russian state disinformation is very effective within Russia itself by forcing the Russian population to accept a distorted reality, it becomes a counterproductive element outside Russian borders (Belousov, 2012) where it no longer achieves its main objectives (Benkler et al., 2018). These contradictions not only substantiate polemics about the ambiguity of Russian disinformation outcomes but also add weight to arguments in favor of the present study. In summary, Russian disinformation in the Baltic States is directed at increasing the populations” distrust in their governments (Lough et al., 2014), promoting the perception of a lack of justice (Paul & Matthews, 2016) or career possibilities (Kuczyńska-Zonik, 2017) within the country, and reinforcing the threat of the imminent military action in the region (Buinauskas et al., 2016).

#### Triggers invasion of the Baltics---escalates quickly

Brent Eastwood 22, Now serving as 1945s New Defense and National Security Editor, Brent M. Eastwood, PhD, is the author of Humans, Machines, and Data: Future Trends in Warfare. He is an Emerging Threats expert and former U.S. Army Infantry officer, January 2022, "Forget Ukraine: Could Russia Invade And Conquer The Baltic States?" https://www.19fortyfive.com/2022/01/forget-ukraine-could-russia-invade-and-conquer-the-baltic-states/ //AShah

We’re Focused on Ukraine But Look Out For the Russian Threat to the Baltics: It was a shot heard around the world in the Russian military analysis community. A RAND Corporation simulated wargame in 2016 concluded that the Russian military could reach the suburbs of the Estonian and Latvian capitals of Tallinn and Riga in less than 60 hours. In the iterations of the exercise, the Estonians and Latvians would need at least seven brigades of troops that include at least three armored brigades to potentially fight the Russians to a standstill.

But it gets worse from here. In another RAND wargame in 2019, the players examined if NATO and Russia would use tactical nuclear weapons during a simulated war in the Baltic states (Estonia, Latvia, and Lithuania). The scenario also had Russian conventional forces over-running capitals in the Balkans and NATO having the last fail-safe option to use non-strategic nuclear weapons.

What Type of Warfare Could the Russians Use Against the Baltics?

A widespread fear is that the Kremlin could use hybrid warfare (conventional and unconventional aspects of power projection) again to annex parts of the Baltics, which would trigger Article V with NATO allies and would require a military response against the Russians from NATO members. A glance at a map will tell you that St. Petersburg is dangerously close to Tallinn, Estonia and Riga, Latvia. But according to General Valery Gerasimov, the Chief of the General Staff of the Armed Forces of Russia, the distinctions between offensive aspects of war and defensive aspects of war are blurring.

Under this Gerasimov Doctrine, the Kremlin then could engineer a Russian hybrid incursion of cyber and information warfare attacks against the Baltics, and these tactics could be made to be seen as a defensive operation. Since the Baltics have ethnic Russians as part of the population, Moscow could employ special operations forces as peacekeepers to protect compatriots. This could happen with an information warfare campaign that would increase the chances for protest and other domestic unrest with ethnic Russians as victims in the Baltics. Then a hybrid operation would ensue to protect ethnic Russians.

According to the two RAND sets of wargames, the Russians would then bring in the heavy armored and mechanized infantry units to “teach the Baltics a lesson.”

#### Russian and Chinese cyber-attacks on critical infrastructure is coming now – laundry list of impacts – NATO cohesion, CI, trust in institutions, Saudi energy.

Dupay et al 21 [Dr Arnold C. Dupuy is a Science Applications International Corporation (SAIC) employee and Chair of the NATO Science and Technology Organization’s program to study hybrid warfare. Dr Dan Nussbaum is a faculty member at the Naval Postgraduate School, the Chair of the NPS Energy Academic Group, and is the Mentor of the NATO Science and Technology Organization’s program to study hybrid warfare. Vytautas Butrimas works in the area of industrial cybersecurity for the NATO Energy Security Centre of Excellence. Alkman Granitsas is a communications consultant at Kyklos Associates with a focus on public policy issues. 1-13-2021, "NATO Review", NATO Review, https://www.nato.int/docu/review/articles/2021/01/13/energy-security-in-the-era-of-hybrid-warfare/index.html, DOA: 7-20-2022 //ArchanSen]

Hybrid warfare is roughly defined as ‘grey area’ warfare, which often exists just beneath the threshold of armed conflict. It is designed to erode public confidence in civil society and democratic foundations, primarily through cyber attacks on critical infrastructure, including energy, or targeted disinformation methods. In this regard, it poses a potential threat to sovereignty, as it gives nations, terrorist organisations and criminal actors relative anonymity via a low-cost, high-yield method to influence the politics and policies of other states.

Russia is one of the most active perpetrators of hybrid warfare and implemented it most effectively in its 2014 illegal annexation of Crimea. The Kremlin continues to use it today, notably in some countries to realise desired political outcomes such as undermining pro-Western governments, dividing and weakening the NATO Alliance, or advancing its own economic interests. China too has recently engaged in cyber attacks and disinformation campaigns aimed at NATO Allies and poses a grave risk to critical infrastructure, including energy infrastructure, as highlighted in the recent NATO 2030 experts’ report.

Ultimately, hybrid warfare challenges to the energy sector have the potential to disrupt the NATO’s political and military effectiveness and cohesion. It will take time and effort to counter these threats, if the Alliance is to address dependencies among its members and act as a platform to build a common picture of complex operational risk and vulnerabilities.

Energy sector increasingly targeted

The use of hybrid warfare is growing. The past decade has seen a dramatic increase in hybrid threats worldwide: from cyber attacks to disinformation campaigns to covert military operations. Threats are becoming more frequent, complex, destructive and coercive. The broader economic and security ramifications of hybrid warfare are evident, especially when applied to the energy sector.

Russia has deployed a range of hybrid threats against the energy assets, policies or supplies of NATO Allies, as well as other countries. It has used political and economic leverage, combined with disinformation campaigns, against Bulgaria and Romania to undermine efforts to reduce their dependence on Russian energy sources. Supply disruptions have been used in the past as well, most famously in the case of Ukraine in 2009, the Baltic states before that and, more recently, against Bulgaria.

Russia has also used its economic clout, combined with political influence, to advance its energy agenda, in Hungary, where the expansion of the Paks Nuclear Power Plant is now underway using Russian energy technology. Likewise, in Germany, Russia has used its commercial and political ties, as well as other suspected malign influence, to advance the controversial €12 billion Nord Stream II pipeline, now nearing completion. Moreover, in 2020, a suspected Russian group, Berserk Bear APT, launched cyber attacks against German energy companies, and has been implicated in previous cyber attacks against German utilities in 2018.

Russian-backed cyber attacks against energy assets have also been identified in a number of other Alliance members, including Poland, Turkey, the United Kingdom and the United States. In some instances, those cyber campaigns have run concurrent with other hybrid threats against energy assets, like malign influence efforts and natural gas supply cutbacks. Taken together, it is clear that – over the past decade and with increasing vigour – Russia has been pursuing a concerted hybrid campaign aimed at undermining the Alliance’s energy security.

Over the same period, among NATO’s partner countries, Russia’s hybrid campaign has been most evident in Ukraine, combining supply disruptions, cyber attacks, economic and political influence, and disinformation efforts to undermine the country’s energy security and sow political instability. The most disruptive effort was Russia’s 2009 interruption of natural gas supplies, but the attacks have continued and become increasingly complex and coercive.

A notable example is the December 2015 Black Energy cyber attack on the western Ukrainian power station, which shut down power for nearly a quarter million residents over a six hour period. This was followed, a year later, with a more sophisticated attack on the power grid supplying electricity to the capital, Kyiv, using CrashOverride/Industroyer malware. While of shorter duration and scope than the previous attack, the effort was far more sinister: it was aimed at compromising electrical safety relays, which are used to protect bulk power equipment. Had it not been detected by analysts, the final attack phase could have led to physical destruction of expensive and difficult-to-replace equipment beyond briefly disrupting power supplies.

Beyond the Euro-Atlantic area, Iran and other suspected states are currently waging a complex hybrid campaign against Saudi Arabia’s energy assets. This campaign may be illustrative of the future of hybrid warfare, particularly in the domain of energy security. Through both covert and overt military operations, and the use of proxy forces, Iran has repeatedly disrupted or otherwise struck Saudi energy infrastructure.

The possible collusion of hostile actors in the ongoing Iranian campaign against Saudi Arabia is of particular concern and may have consequences for NATO Allies. Specifically, the 2017 cyber attack on the Petro Rabigh complex, which resulted in a costly shutdown and forensic clean-up of the facility and very nearly resulted in an uncontrolled gas release and explosion. Despite initial speculation that Iran was uniquely responsible for the dangerous Triton malware used in the attack, the United States has since concluded that the malware was developed by Russia and imposed sanctions on the research institution connected with its development. The malware has also been implicated in attacks on energy companies in the United States.

Other suspected measures in Iran’s campaign include two drone strikes by Iran’s Houthi allies on Saudi refineries, covert attacks on two Saudi registered oil tankers in the Persian Gulf and, most recently, attacks on two foreign-flagged tankers at Saudi ports on the Red Sea. Notably, the drone strike on the Saudi Aramco Abqaiq refinery in late 2019, which was claimed by Houthi forces, provided Iran with deniability and helped expose air defence weaknesses in Saudi Arabia.

#### CI – extinction.

Delacourt 22 [[Ted P. Delacourt](https://www.hstoday.us/author/tdelacourt/) 02-01-2022, "Cyberattacks on Critical Infrastructure as the New WMD", Hstoday, https://www.hstoday.us/featured/cyberattacks-on-critical-infrastructure-as-the-new-wmd/, DOA: 7-20-2022 //ArchanSen]

Should the acronym WMD, which stands for “Weapons of Mass Destruction,” be updated to “Weapons of Mass Disruption?” I think it is a timely question in this Digital Age as we connect and integrate billions of new digital devices into our lives and business processes and when a cyber-attack against one supply chain provider can lead to cascading effects on entire communities across the globe. Cyberattacks on Critical Infrastructure (CI) can cause mass economic and societal impacts. Fewer strategies than cyber-attacks can offer better plausible deniability and can cause greater anxiety and instability to our society than targeting the systems and networks that enable our day-to-day activities. Consider that 20 years ago terrorists killed 3,000 Americans and disrupted the entire U.S. and global economies with only four planes. Given the growth and ubiquity of technology today we must consider how the exponential growth of cyberattacks on CI might be similarly leveraged by adversaries and criminal actors as Weapons of Mass Disruption, the new WMD.[1]

Cyberattacks take many forms, often progressing through multiple phases as they escalate in severity. Malicious actors often initiate a network intrusion through phishing campaigns or the purchase of compromised user credentials on the dark web. What begins as the hijack of a single user profile expands in severity. Intruders move laterally across internal systems, conducting surveillance and gathering intelligence on network environments before escalating to data theft, service disruptions, and ransomware extortion.

The goals of these actors may be both strategic and economic in nature, and targets may be government and/or the private sector. Cyberattacks perpetrated on CI elements develop into the new WMD when the intended and unintended consequences cause widespread damage and societal impacts. A disruption of essential services, even if brief, can occupy significant civilian and military resources in a region or entire country.[2]

#### Specifically, Lithuania facing onslaught of intense Russian hacks

Manthorpe 6-28 (Rowland, studied History at Cambridge and Political Theory at the London School of Economics, and has been awarded the Ben Pimlott Prize for Political Writing by the Guardian and The Fabian Society. Rowland is Technology correspondent, reporting on the many areas tech is transforming lives. “Could the Russian cyber attack on Lithuania draw a military response from NATO?”, https://news.sky.com/story/could-the-russian-cyber-attack-on-lithuania-draw-a-military-response-from-nato-12641986)LR

**A NATO member is under attack.** The NATO member in question is the Baltic state of **Lithuania**, which was **targeted on Monday by Russian hackers.** According to the hackers, the attack is still going on. Transport and media websites have been hit, as have the websites of various state institutions such as the Lithuanian tax service, which had to pause its operations yesterday. A Russian hacker group known as Killnet claimed responsibility for the attacks, claiming on its Telegram channel that the attack was retaliation for Lithuania's decision to stop the transit of some goods to the Russian territory of Kaliningrad on the Baltic coast. The politics of this situation are extremely complicated. Kaliningrad is Russian-owned, but it isn't connected to the main body of Russia - it's a small piece of Russia surrounded by NATO countries. The Lithuanian government says it is simply enforcing European Union sanctions on goods, but Russia has responded with outrage, saying it is being stopped from accessing its sovereign territory**. Russia promised to respond** in a way **that would "have a serious negative impact on the population of Lithuania"**. Then, a **few days later, came this cyber attack**. Does that mean Russia attacked a NATO member? Not so fast. For a start, the group that claimed responsibility denies any connection to the Russian state, saying it is "not affiliated with any law enforcement authorities". The Russian government has long used third-party criminal groups to conduct hacks and cyber attacks, so it would not come as a surprise if it was involved. Nevertheless, on the surface at least, its hands are clean. Then there's the nature of the attack. Reports so far suggest that it's a distributed denial of service (DDoS) attack, a crude attack which involves throwing huge amounts of traffic at a website until it is forced offline. The attack has been described as "massive", which is technically true, because in order to work a DDoS attack has to be large, but that doesn't mean it will have a massive effect. DDoS attacks are so common that most websites nowadays have protection against them as standard. Even if an attack does work, it won't steal any data. It's a blunt force instrument, little more. Yet that does not mean we aren't moving towards that point, nor that a cyber attack cannot lead us there. Another way in which cyber attacks are different to physical attacks is that once they are started they can spiral out of control. Unlike a bomb or a bullet, a virus can spread in ways that even its makers don't intend. Almost exactly five years ago, the costliest ever cyber attack was launched: a malware attack called Not Petya. It is believed to have begun when Russian operatives infected a small piece of Ukrainian accounting software, intending to disrupt Ukrainian businesses. But from there it spread to companies around the world, including shipping giant Maersk and food conglomerate Mondelez. By the time it was done, Not Petya had caused $10bn in estimated damages.

#### Draws in NATO and the US

Zemelyte 6-27 (Beatrice, BA in Administration, Human Resources, and Marketing at University of Vermon, interviewing Agnia Grigas - Dr. Agnia Grigas is an energy and political risk expert. She specializes in energy and foreign policy of the U.S. and Eurasia including Europe, Russia, China, the states of the former Soviet Union, and the Baltic States. She has fifteen years of experience as a business development and political risk advisor to corporations and government agencies. She is an author of three critically acclaimed books The New Geopolitics of Gas (Harvard University Press, 2017), Beyond Crimea: The New Russian Empire (Yale University Press, 2016), and The Politics of Energy and Memory Between the Baltic States and Russia (Ashgate 2013). Dr. Grigas graduated cum laude with a BA in economics and political science from Columbia University, New York, NY and earned her Master’s and Doctorate in international relations from the University of Oxford, UK where she is an alumna of St Antony’s and Brasenose colleges. “Kaliningrad standoff could reveal if Russia wants to ‘escalate’”, https://www.aljazeera.com/news/2022/6/24/achilles-heel-of-nato-tensions-amid-kaliningrads-transit-ban)LR

Al Jazeera: Russia has said Lithuanian citizens will “feel the pain” over Kaliningrad. How might Moscow respond? Grigas: Russia could enact its own sanctions on the sale of goods to Lithuania. The key Russian exports are oil and gas, and electricity, and Lithuania has already made a decision much earlier before this conflict, that it will not be purchasing any Russian energy sources. There could be a question of fertilisers and other elements but there is already a broad blanket of European sanctions against Russian goods. I view Russia’s statements more as threats and posturing for the Russian domestic audience because a lot of [Russian President Vladimir] Putin’s statements tend to be aimed to show the resolve and the strength of the Kremlin, rather than necessarily specifying any sort of actions they would take or for the external audience. What is concerning is that Russia used or the Kremlin use the terms that Lithuania has enacted a blockade, either the word choice is important, because blockade could be perceived as a military already action, and therefore, Russia could try to, you know, justify some sort of [military action], as well.” Al Jazeera: How do you think the Kaliningrad situation can impact the war in Ukraine? Grigas: I think this situation in Kaliningrad will show whether Russia is willing to escalate further this conflict against the West, the European Union and NATO. Al Jazeera: The United States has said that it will stand behind Lithuania and its NATO commitments to defend it … Grigas: NATO, the United States and European Union countries have been very cautious not to get involved in this war. There’s a real fear of potential escalation of conflict with Russia directly because one, Russia remains a nuclear state. Second, because of the fact that it’s controlled essentially by a single man with a very small circle of advisers, who has essentially a free hand to take whatever decisions he may wish. Al Jazeera: Lithuania and Russia already had weak diplomatic relations, and the war in Ukraine has worsened them. How will their ties be affected by the ban? Grigas: Lithuania has been a very vocal supporter of Ukraine since the very start of the war this February and, frankly, since Russia’s occupation of Crimea [in 2014] and the initial invasion of the Donbas. Earlier this summer, Russia and Duma deputies were discussing whether they should revoke Lithuania’s independence that was agreed to by the Soviet Union in 1991. This is part of kind of a broader package of the Kremlin’s threats on a smaller neighbouring country. I don’t think Lithuanian-Russian relations will improve in the near future. Frankly, European and Russian relations will not improve in the near future, nor will NATO and Russian relations, particularly as long as the ongoing war in Ukraine continues.

#### Baltic State Utility to US

Banka 2022, (Andris Banka , Journal of Transatlantic Studies volume 20, pages161–183 (2022), Published 4/5/2022 “Neither reckless nor free-riders: auditing the Baltics as US treaty allies” https://link.springer.com/article/10.1057/s42738-022-00096-3)

A great deal of scholarly literature has treated Baltic States’ physical proximity to Russia as their Achilles heel. The conventional wisdom holds that due to the force imbalance in the region, which heavily favours the Russian side, Baltic republics are hard to defend territories.Footnote82 While this assumption is certainly valid, there is, however, a flip side to this predicament. Situated at a geopolitical crossroads, these small nations are in an advantageous position to produce valuable insights into Kremlin’s statecraft. As James Carafano suggests: “To a major power, a country’s greatest asset might be its map coordinates rather than the size of its arsenal or bank account”.Footnote83 Similarly, Brands and Feaver have noted that some of the most valued US intelligence assets stem from allied partners “geographical capability” and “proximity to the theater of interest”.Footnote84 Lacking in material power resources, the Baltic States, within the past decade, have made a concerted effort to set up “knowledge hubs” that excel in analysing their much larger eastern neighbour. Having been subjected to Russian-directed gray zone tactics for decades, the Baltics have amassed valuable regional expertise. Testifying before the US Committee on Foreign Affairs, a prominent Russia-observer explained: “They [the Baltics] see things that we don’t see. They can go to places that we don’t go. They understand things that we don’t in cyber and intelligence”.Footnote85 Retired Lieutenant General Ben Hodges, who commanded the US Army Europe, concurs by emphasizing that the Baltic republics, due to their location, “know more what is happening in Russia, than any American will ever know”.Footnote86 Indeed, the Baltics fill in critical gaps in fields such as cyberwarfare, intelligence gathering, and disinformation, actively sharing this “know-how” with their US counterparts. The following details such contributions The Republic of Estonia was the first known victim of a state-directed cyberattack. The 2007 incident, widely attributed to the Russian Federation, for weeks incapacitated Estonian governmental structures. Somewhat paradoxically, in the long run, the event turned out to have a positive impact as it propelled the nation of 1.3 million people to treat the cyber domain as an intricate part of its national security. Subsequently, the country set up the Tallinn-based NATO Cooperative Cyber Defence Centre of Excellence. According to the Estonian President Kersti Kaljulaid, this was a smart way for a small country to demonstrate its contributions to allies.Footnote87 Understanding that it has little to offer in hard-power deliverables, Estonian leadership chose instead to focus on the cyber domain. In the words of Kaljulaid’s predecessor, Toomas Ilves, the IT field served as “the great equalizer”, allowing a small nation to contribute considerably more than one “would expect by looking at the map, population, and GDP per capita”.Footnote88 Today, Estonia has a well-established reputation among its peers as the lead authority for devising cybersecurity-related solutions. When it comes to countering cyber threats, Tallinn and Washington have forged a close bilateral relationship on various departmental levels. In 2020, the two governments set up a joint cyber-threat intelligence-sharing platform.Footnote89 In addition, the US Army and Estonia’s Ministry of Defence entered into an agreement for collaborative research on cyber defence matters.Footnote90 Such joint initiatives have already borne fruit. In the run-up to the 2020 US Presidential election, in order to learn more about Russian hacking methods, the USA dispatched its cyber force operatives to Estonia.Footnote91 For the USA, this allowed to observe the work of Kremlin-linked agents and bolster its own election defences. Commenting on this deployment, US Deputy Assistant Secretary of Defense for Cyber Policy pointed out: “Cyber is a team sport—when it comes to halting threats from cyberspace, no one can go it alone”.Footnote92 Such operations illustrate how small states can amplify the reach of the USA and effectively complement its capabilities. Estonian authorities have regularly received praise for the provision of such services. James Mattis, US Secretary of Defense in the Trump administration, upon meeting his Estonian counterpart underscored that Washington highly appreciates Estonian leadership in this new area of competition, and that its positive example speaks to the fact that the size of the country does not necessarily determine its contributions to collective security.Footnote93 In a similar vein, NATO Secretary-General Jens Stoltenberg has spoken highly of Estonia for its efforts in training and educating NATO military staff.Footnote94 After being the first victim of a Russian-linked cyberattack, Estonian leadership managed to turn the incident into a certain asset. By studying its lessons and building resilience, it gradually emerged as the lead cyber-knowledge exporter. For many, Russia’s abilities to effectively plant disinformation campaigns overseas came into sharper focus during the 2016 US presidential election. For the Baltics, however, such malign interference and attempts to sow societal divisions were hardly anything new. Lawmakers in the region have been sounding the alarm about it ever since regaining independence in the early 1990s. However, it was only in 2014 that Latvia opened the NATO Centre of Excellence devoted to the exploration of such issues. Its central analytical focus is on tracking and analysing Russia’s digital footprint. Since its establishment, the research institution has produced innovative studies regarding information-warfare efforts employed by Kremlin-linked actors and experimental takes on societal vulnerabilities. Such analysis has often been shared with the US government via testimonies before the US Senate Select Committee on Intelligence and briefings with the US military staff.Footnote95 Commenting on the centre’s work, a senior US Congressman pointed out that because of their “first-hand experience with the Soviet Union and Putin’s Russia”, the Baltics have become “a valuable source of insight” for the US government.Footnote96

#### Trust in institutions – extinction.

Tisdall 22 [Simon Tisdall is a foreign affairs commentator. He has been a foreign leader writer, foreign editor and US editor for the Guardian, 1-9-2022, "The epic struggle for America’s soul is just getting started", Guardian, https://www.theguardian.com/commentisfree/2022/jan/09/the-epic-struggle-for-americas-soul-is-just-getting-started, DOA: 7-20-2022 //ArchanSen]

A new USA Today/Suffolk University poll found eight in 10 Republicans, Democrats and independents are worried about the future of American democracy. But they disagree over the causes – and who’s to blame: 85% of Democrats call the Capitol Hill rioters “criminals”; two-thirds of Republicans believe “they went too far but had a point”.

“Only free and fair elections in which the loser abides by the result stand between each of us and life at the mercy of a despotic regime,” warns Harvard law professor Laurence Tribe. But increasingly, for today’s politicians, honourable defeat is a wholly foreign concept.

This chronic loss of institutional trust and credibility, also tainting a politicised, conservative-dominated supreme court, reflects a society more openly riven by longstanding cultural, racial and religious animosities – and one in which income, wealth and health inequalities are growing. These divisions are in turn wilfully exacerbated by rightwing broadcast and online media, bloggers and internet trolls.

A Republican party mostly in thrall to Trump’s lies, delusions and conspiracy theories is creating a world of “alternative facts”, says columnist Thomas Friedman. If they succeed in replacing truth, “America isn’t just in trouble. It is headed for what scientists call ‘an extinction-level event’”.

Jedediah Britton-Purdy, a Columbia law professor, is similarly apocalyptic. “One thing Democrats and Republicans share is the belief that, to save the country, the other side must not be allowed to win … Every election is an existential crisis,” he wrote.

“We should stop underestimating the threat facing the country,” a grim New York Times editorial thundered last week. “January 6 is not in the past; it is every day. It is regular citizens who threaten election officials, who ask ‘when can we use the guns?’, who vow to murder politicians who dare to vote their conscience. It is Republican lawmakers scrambling to make it harder for people to vote and subvert their will if they do. It is Trump who stokes the flames of conflict.” Democracy, it said, was in “grave danger”.

Systemic violence that overwhelms conventional politics may be near at hand. “We are closer to civil war than any of us would like to believe,” says Barbara Walter, a California politics professor.

No one is talking about a remake of the 1861-65 US civil war. Instead, as in Ukraine or Libya, an “open insurgency”, as defined by Walter, would probably involve (at least initially), disparate militias and their supporters pursuing forms of asymmetrical warfare – typically terrorist acts, bombings, assassinations, kidnappings. That said, worrying echoes of Confederate-era secessionism are once again heard in Texas and elsewhere.

When the warlike rhetoric of Charlottesville-style paramilitary white supremacists, the high nationwide incidence of gun ownership and, for example, worries about far-right cells within the US military are factored in, civil war scenarios do not appear so implausible.

“Only a spark is needed, one major domestic terrorist event that shifts the perception of the country,” analyst Stephen Marche wrote last week. Marche quotes a military history professor and Iraq war veteran, Col Peter Mansoor, who tells him: “It would not be like the first civil war, with armies manoeuvring on the battlefield. I think it would very much be a free-for-all, neighbour on neighbour, based on beliefs and skin colours and religion. And it would be horrific.”

## Modelling Advantage

#### Scenario one is warming—

#### NATO involvement is key to overcome dependence

ÇAlışMa Grupları, Diplomasigeneluluslararası, which is a very important job in another language İLişKiler· 4-28- 2022·, "The Energy Security of the Baltic States and the Tensions with Russia," TESAD, https://www.tesadernegi.org/the-energy-security-of-the-baltic-states-and-the-tensions-with-russia.html//DG

The last term applies to the interconnection between the Baltic States and Russia as the Baltics are considered vulnerable and a trade war could drag them down in a crisis[45]. Since the Baltic market is not economically important to Russia, the interdependence is considered asymmetrical. Russian exports for the year 2020 to Latvia were 2.23B, Estonia $2.59B, and Lithuania $2.39B[46]. Nevertheless, from the opening of the Balticconnector and other interconnections belonging to the European network the region plays an important role in gas and petroleum transit, ensuring the uninterrupted flow of energy to further European destinations. Consequently, the Kremlin started to look around for solutions and has developed a strategy comprising the construction of alternative routes, namely the Nord Stream 1 and 2, the Turkish Stream and the Power of Siberia pipelines.

However, the complex situation must be framed inside a broader strategic vision according to Keohane’s and Nye’s interdependence theory. Russian weight in the Baltic energy security undergoes military security conditions. The Baltic States are part of the eastern flank of NATO, therefore their integration into the Russian energy infrastructure is meant to balance the presence of the Western military alliance in the region[47]. Moreover, the Baltics register a high presence of Russian immigrants in their populations, thus energy is used as a weapon to prevent any kind of discrimination.

The request of the Estonian Defence minister for a strengthening of NATO’s presence in the Baltics following the outbreak of the Russian-Ukrainian conflict in 2022 reflects well the interdependence hypothesis. Estonia, likewise, its neighbours, fears the extension of the conflict to the area and the possibility of retaliation in the energy sector, as the country has engaged itself actively in the reception of war refugees from Ukraine[48]. According to the Bank of Estonia, the outbreak of war has influenced markets, prices of natural gas and electricity are increasing, and households’ consumption is expected to reduce in the short term. Therefore, the Estonian government decided to place natural gas and heating under a price ceiling until spring 2022[49]. Lithuania on its side is bringing forward the GIPL project with Poland and is looking forward to opening the pipeline ahead of schedule, on May 1st. The three countries foresee closer regional and European cooperation to reduce their dependence.

In the past, Russia could benefit from the European uncertainty due to the different levels of European involvement in the matter and the controversy in the support of stronger sanctions. But a comprehensive energy network has been developed in the past twenty years and now the European Union presents itself as a single and active actor in the international environment, that stands for the democratic values and is ready to defend itself against external claims of special interest zones in the former Soviet space[50]. For the Baltic States, this means knowing that they can fully lean on Western support in asserting their own sovereignty.

Therefore, to reinforce its self-determination, the European Union launched the REPower plan in March 2022, aiming at phasing out the fossil fuels import dependence from Russia. The strategy requires the almost complete filling up of the capacity gas stock storage before winter, the replacement of gas in heating and power generation and more renewables investments[51].

#### Baltic renewables k2 european green energy transition

Lukas Trakimavičius, 3-19-2021, Trakimavičius works at the Research and Lessons Learned Division of the NATO Energy Security Centre of Excellence "The untapped green energy potential of the Baltic States," euractiv, https://www.euractiv.com/section/energy/opinion/the-untapped-green-energy-potential-of-the-baltic-states//DG

As the global energy transition gathers speed, the Baltics may not seem like its obvious frontrunners. Despite making great strides in making their energy systems cleaner, fossil fuels still remain a staple of their energy diet. However, growing evidence suggests that the Baltics have a massive offshore wind energy potential, which could have a game-changing effect for the entire region. Chances are, wind turbines could not only propel the Baltics to the forefront of the energy transition, but also to the ranks of clean energy exporters. As things stand, few would argue that the Baltics are on the cutting edge of the clean energy transition. Like most of their European peers, they get the bulk of their energy from fossil fuels such as oil and natural gas. These are either imported from far abroad or, as is the case with Estonian oil shale, mined from deep underground. Meanwhile, renewables such as onshore wind, solar or hydropower still account for a tiny fraction of their overall energy needs. In 2019, these energy sources met some 2.6 percent of [Lithuania](https://www.iea.org/countries/lithuania)’s, 4.6 percent of [Latvia](https://www.iea.org/countries/latvia)’s and 1.3 percent of [Estonia](https://www.iea.org/countries/estonia)’s total primary energy demand. Granted, the overall share of renewables is vastly greater once biomass is added into the mix. Yet, some scientists [argue](https://ec.europa.eu/jrc/en/publication/eur-scientific-and-technical-research-reports/use-woody-biomass-energy-production-eu) that fuels such as firewood or wood pellets may not be the most environmentally sustainable sources of energy. However, what the Baltics lack in fossil fuels, they make up for with an abundance of wind in the Baltic Sea, which can be harnessed and converted into electricity. Though currently none of the Baltics have any windmills in the open seas, all three have major offshore wind plans for the future. Lithuania, for example, intends to [have](https://enmin.lrv.lt/en/news/offshore-wind-another-direction-of-renewable-energy-to-strengthen-local-power-generation-in-lithuania) at least 700 megawatt (MW) of offshore wind farms in operation by 2030. Latvia and Estonia are also eying to co-develop a [joint](https://www.windpowermonthly.com/article/1690879/estonia-latvia-sign-pact-1gw-offshore-wind-farm) 1,000 MW wind farm in the Gulf of Riga. On top of that, Estonia [wants](https://news.err.ee/1149566/dutch-company-van-oord-buys-stake-in-saare-wind-energy) to have a 1,000 MW offshore wind park near the island of Saarema by 2028, in addition to a slew of other projects that are under [consideration](https://www.windpowermonthly.com/article/1690879/estonia-latvia-sign-pact-1gw-offshore-wind-farm).All of this sounds great, but it could just be the beginning. According to a recent WindEurope [study](https://windeurope.org/wp-content/uploads/files/about-wind/reports/WindEurope-Our-Energy-Our-Future.pdf), the Baltic Sea could be the next big thing for Europe’s energy transition. It is estimated that Lithuania [could](https://windeurope.org/wp-content/uploads/files/about-wind/reports/WindEurope-Our-Energy-Our-Future.pdf) have up to 3,600 MW, Latvia up to 2,900 MW and Estonia up to 1,500 MW of offshore windfarms by 2050. If this generation capacity could be met, the study claims that the Baltics could potentially [export](https://windeurope.org/wp-content/uploads/files/about-wind/reports/WindEurope-Our-Energy-Our-Future.pdf) around half of their offshore wind electricity to neighboring states. Obviously, it is difficult to say with certainty just how much electricity would the Baltics be able to export and others would like to import. After all, to get to a zero-carbon future, the Baltics and their neighbors will have to [undergo](https://www.weforum.org/agenda/2020/04/can-electricity-decarbonize-the-energy-sector/) tremendous changes by 2050. Not only will they have to make energy use more efficient, but they will also have to decarbonize and electrify large portions of their economies. Still, if the Baltics would harness their full offshore wind potential and would continue to develop other renewable sources of energy, there are few doubts that a good chunk of their electricity might still be available for export. To get more bang for the buck, the Baltics could also take some of this newfound electricity and transform it into green hydrogen using a process known as electrolysis. Green hydrogen could be used for manufacturing, transport, heating or [converted](https://www.scientificamerican.com/article/solar-and-wind-power-could-ignite-a-hydrogen-energy-comeback/) back into electricity to back up the grid. Or it could simply be exported to neighbouring states. This step would prevent excess electricity from being wasted and also help decarbonise those sectors of the economy where electrification is difficult.

#### European transition checks warming---else, all other renewables fail

EEA, European Environment Agency 8-1-2017, "Energy and climate change," European Environment Agency, https://www.eea.europa.eu/signals/signals-2017/articles/energy-and-climate-change//DG

The global climate is changing and that is posing increasingly severe risks for ecosystems, human health and the economy. The EEA’s recent assessment ‘[Climate change, impacts and vulnerability in Europe 2016](http://www.eea.europa.eu/publications/climate-change-impacts-and-vulnerability-2016)’ shows that Europe’s regions, too, are already facing impacts of a changing climate, including rising sea levels, more extreme weather, flooding, droughts and storms.

These changes are happening because large amounts of greenhouse gases are released into the atmosphere as a result of many human activities worldwide, including, most importantly, burning fossil fuels for electricity generation, heating and transport. Combustion of fossil fuels also releases air pollutants that harm the environment and human health.

Globally, the use of energy represents by far the largest source of greenhouse gas emissions from human activities. About [two thirds of global greenhouse gas emissions](http://www.iea.org/publications/freepublications/publication/CO2EmissionsfromFuelCombustion_Highlights_2016.pdf) are linked to burning fossil fuels for energy to be used for heating, electricity, transport and industry. In Europe, too, the energy processes are the largest emitter of greenhouse gases, being responsible for 78 % of total EU emissions in 2015.

Our use and production of energy have a massive impact on the climate and the converse is also increasingly true. Climate change can alter our energy generation potential and energy needs. For example, changes to the water cycle have an impact on hydropower, and warmer temperatures increase the energy demand for cooling in the summer, while decreasing the demand for heating in the winter.

Global efforts so far to mitigate climate change culminated in the [Paris Agreement](http://unfccc.int/paris_agreement/items/9485.php) in 2015. Through the agreement, 195 countries adopted the first-ever universal and legally binding, global climate deal. The target of the agreement — limiting the global average temperature rise to well below 2 °C, while aiming to limit the increase to 1.5 °C — is ambitious and cannot be achieved without a major overhaul of global energy production and consumption.

To support the global climate agenda, the EU has adopted binding climate and energy targets for 2020 and proposed targets for 2030 as part of its overall efforts to move to a low-carbon economy and to cut greenhouse gas emissions by 80-95 % by 2050. The first set of climate and energy targets for 2020 includes a 20 % cut in greenhouse gas emissions (compared with 1990 levels), 20 % of energy consumption coming from renewables and a 20 % improvement in energy efficiency. Based on the current proposals in discussion in EU institutions, the next milestone of 2030 pushes these targets to a 40 % cut in emissions, 27 % of energy coming from renewable sources and a 27 % improvement in energy efficiency (or 30 %, as recently proposed by the European Commission) compared with baseline.

#### Warming causes extinction – adaptation doesn’t assume tipping points and corporations prevent intervening actors.

John Coviello 21 [John Coviello, 12-18-2021, Author of [One Last Breath: A Look Back at 200 Years of Global Warming](https://www.goodreads.com/book/show/54327991.One_Last_Breath_A_Look_Back_at_200_Years_of_Global_Warming). Winner of the prestigious 2021 Book Excellence Award for Sustainability. Are Humans Facing Near-Term Human Extinction Due to Global Warming? Soapboxie, https://soapboxie.com/social-issues/Are-Humans-Facing-Near-Term-Human-Extinction-Due-to-Global-Warming, DOA: 12-26-2021 //ArchanSen] \*edited for sexist language

While some scientists started raising concerns about the burning of fossil fuels eventually warming the Earth’s atmosphere as far back as the middle 20th century, a consensus among scientists that global warming is a problem we have to address didn’t form until the later part of the 20th century. Now that we’re progressing through the 21st century, why are some in scientific circles raising concerns about our near-term survival as a species? In recent years, the effects of global warming have become exceedingly extreme. In fact, from record-breaking heatwaves to unprecedented forest fires to melting polar ice sheets, the effects of global warming are occurring faster than the scientific community had projected they would just a decade or two ago. The concern about our viability as a species on Earth is due to the fast-developing effects of global warming. If we don’t address the causes of global warming or take mitigative actions, it could transform into runaway global warming that would heat up the Earth so rapidly that humans and many other species will likely be imperiled. Many scientists wrongly had confidence that [hu]mankind would come to its senses when faced with the stark reality that our survival as a species is threatened and we’d collectively take actions to avert catastrophic global warming by discontinuing our burning of fossil fuels and replacing them with renewable non-carbon energy sources. However, despite some tepid efforts to cut carbon emissions, such as the 2016 Paris Agreement, it appears that due to a combination of ignorance and a concerted effort by the fossil fuels industry to stop any efforts to move away from carbon-based products, we will likely not address our continuing release of global warming gases into Earth’s atmosphere until it’s too late and the global warming we’ve experienced in recent decades transforms into irreversible and catastrophic runaway global warming. This will occur because human-caused global warming will eventually trigger natural climate warming feedback loops to take over. At that point, global warming will be like an unstoppable runaway train, as the Earth’s atmospheric temperatures rise to life-threatening levels. These warming feedback loops include such things as releases of global warming gases from melting polar ice sheets and from frozen methane deposits beneath the oceans, as well as the loss of polar ice causing the Earth to absorb more of the sun’s heat energy. All of which will cause additional warming, which then results in additional releases of global warming gases that will cause additional global temperature rises in an unstoppable loop that will continue until the planet is warmer than it has been in many millions of years (long before humans existed). Such rapid and uncontrollable warming of Earth’s atmosphere could warm the planet by 4 to 5 degrees Celsius (7 to 9 degrees Fahrenheit) within the current century and perhaps eventually lead to a planet that is 8 to 9 degrees Celsius (14 to 16 degrees Fahrenheit) warmer than it was before humans started burning fossil fuels in large quantities starting in the 19th century. Some might wonder, what’s the big deal if the planet is 4 to 5 degrees Celsius or even 8 to 9 degrees Celsius warmer than it has been as humans evolved on Earth? After all, many parts of the planet routinely experience temperature swings of this magnitude on a daily or weekly basis. There are several ways that rapid global warming on a planetary scale could threaten human survival. Warming is not evenly distributed. Some areas, including currently farmable land, will warm well in excess of the global average, which would lead to desertification and crop failures. This would obviously imperial humans due to massive food shortages. Oceans, another major source of food that humans need to survive, are impacted by rising global temperatures, as higher ocean temperatures lead to acidification of ocean water, which will eventually lead to massive die-offs of sea life that provide much-needed food for humans. Water resources will completely dry up in many arid parts of the world, making those areas uninhabitable. Dwindling food and water resources will inevitably lead to wars between competing nations that could be catastrophic. Humans can’t survive at wet-bulb temperatures above 35 degrees Celsius (95 degrees Fahrenheit), even in the shade, as the human body loses its ability to cool itself off. Higher global temperatures and the higher humidity levels that will occur with the higher temperatures could make large parts of the Earth uninhabitable due to wet bulb temperatures that are lethal. Would Runaway Global Warming Actually Lead to Human Extinction? It’s a very big step go from runaway global warming to the extinction of all human beings on Earth. Humans possess the intellectual skills necessary to design and build technologies that can help us adapt to climate change. We’re also able to move to places with more hospitable climates. However, some scientists are concerned that humans will not have time to adapt to the quick pace of runaway global warming and some of the impacts will be too harsh for us to survive. If farmlands and oceans are no longer capable of providing food for humans, where will we turn to obtain life-sustaining food? It is possible that humans could migrate towards the poles and try to farm on land in those areas that is freed up from the ice. However, it is unclear if the currently frozen areas in and around the polar regions will have topsoil suitable for farming. What about freshwater fish? Unfortunately, freshwater lakes and rivers will also undergo acidification that will likely wipe out most or all fish species that can provide humans nourishment. Our only hope might be some sort of synthetic food that is created in factories using basic elements (a technology that is certainly viable). There will be other life-threatening factors that humans will face in a fast warming world. Massive fire balls from methane releases will create havoc for humans. These fireballs will start enormous forest fires driven by the warmer and in many places a more arid world, which will cause turmoil for humans. A lack of freshwater in areas that undergo desertification will make survival impossible in such areas. Wars over dwindling resources will be fought out of desperation and could end in catastrophe. The stress of a warmer world will weaken human immune systems. If industrial society collapses or is greatly reduced, healthcare and medicines might become very limited, lowering life expectancy dramatically. Humans that survive all the dangers associated with runaway global warming might succumb to pandemics that will likely sweep the world as opportunistic pathogens take advantage of weakened human systems and cause a large loss of life in the remaining human populations.

#### Scenario two is Taiwan—

#### 5G cyber is the new battlefield, mutual cooperation between US-NATO with the Baltics key to combat China and Russia

Wierenga 22 (Louis Wierenga Junior Research Fellow, Johan Skytte Institute of Political Studies, University of Tartu | Lecturer in International Relations, Department of Political and Strategic Studies, Baltic Defence College. “Cybersecurity and Hybrid Threats in the Digital Baltic states: A state of the art”, https://www.baltdefcol.org/files/files/publications/Hybrid%20Threats\_LIIA.pdf)LR

In light of power competition vis-à-vis cooperation with the US, NATO, and the EU, and small states standing up to larger powers with nefarious intentions, the drawback is that no entity is capable of defeating all cyberattacks; rather, in order to succeed in cyberspace, the key is learning how to adequately cope.24 When it comes to information warfare, and one of the reasons for which it is so dangerous, is that the antagonist need not win – they succeed if they are able to successfully cloud the issue.25 It is no secret that **Russia has waged** **numerous information warfare campaigns in the Baltics** and show no sign of giving up. Recommendations and policy developments Keep on the cusp of cyber hygiene and widely promote amongst citizens: General H.R. McMaster notes the importance of American efforts to conduct reconnaissance in cyberspace and preempt attacks.26 Strive to continuously be one step ahead of hackers. Although this is a daunting, if not (nearly) impossible task, it is one which would involve both governments and the general public. One aspect which has greatly contributed to the success of Estonia in becoming a world leader in cyber defence is investing in people.27 Promoting cyber hygiene is one aspect at which Estonia excels. Raising further awareness about media literacy to combat disinformation and misinformation also helps to win the battle against information warfare. McMaster also advocates for the US to learn from countries which were on the receiving end of Russian aggression.28 As one of the strengths which Estonia possesses is its investment in people, Estonia is a success story in cyber and IT education and training, ranging from kindergarteners to the elderly.29 In an increasingly multipolar world order**, the rise of China presents a serious security challenge** to Europe and the Transatlantic alliance and can be seen on a number of fronts. One of the most pressing, especially when it comes to cybersecurity, is 5G. If seen through the lens of ‘the West’, then a united front should consist of the US and NATO, plus PfP countries, along with the EU in cyber policy. When it comes to 5G, this is especially important. The Baltic states have taken strides to become leaders in 5G policy and can use this opportunity to take a leading role in a Western front in the battlegrounds for 5G policy. Keeping focus on both China and Russia as threats to the security of NATO and the EU: For valid reasons – both historical and contemporary – the Russian Federation is identified as the primary security threat to the 3 Baltic states. The most contemporary events in the neighborhood do not indicate any change in the consistency or persistence of the threat, nor its digital nature. Cyber and hybrid threats directed towards the Baltic states from the Russian Federation will not cease and military, government, and civilian entities need to continue with vigilance, adapt to the rapidly changing nature of cybersecurity and cyberwar, as well as anticipate future changes, staying ahead of the curve. However, despite the very valid concerns over Russian cyber activity, the Baltic states should not neglect such concerns as they relate to China. Indeed, as aforementioned, the Baltic states, especially Lithuania, have taken a firm stance towards China, in cyberspace and beyond, and should continue to use their growing digital prowess to expand their influence in the EU and NATO. Lithuania, under the leadership of Foreign Minister Gabrielius 63 Landsbergis, has increasingly stood up to China.30 Minister Landsbergis’s stance towards China led to him being named as one of Politico’s ‘most influential people in Europe’ – and the only one to make the list from any of the Baltic states.31 Latvia has called upon China to respect the rules of international cyberspace.32 It should be noted that this is certainly not the first time that leaders from the Baltic states have appeared on similar lists, granting small states representation on lists where the usual larger powers within Europe enjoy substantial representation. Such leadership should be emulated, and the digital advances made by the Baltic states provides an ideal way to achieve this, as many countries look to the Baltics as digital leaders. Demonstrating leadership to allies: If ever there was a time, as well as a concrete area for the Baltic states to showcase their strengths as small states, demonstrating leadership in the cyber and tech fields presents the perfect opportunity. Estonia has been the Baltic champion for cybersecurity and e-governance. Lithuania, and to a lesser extent Latvia have shown signs of catching up. Much like offline matters, the three Baltic states use opportunities to meet with US and EU leaders to highlight the dire security situation which the Transatlantic alliance faces from a resurgent Russia – they know from experience and contemporary matters. As the security of cyberspace is one of the acute questions of global politics this century33, cybersecurity and matters of digital warfare will be issues which merit pressing resolve, which is constantly changing. Being on the cutting edge will require countries to remain that way. While member of the United Nations Security Council for the first time, Estonia made cybersecurity a priority, along with the overall security of the region.34 As well, when a member of the UN Security Council, Estonia made it a point to align with the US and the UK to call Russia out over a cyberattack directed at Georgia.35 Latvia and Lithuania have also been active on such fronts. In 2021, Latvia signed an agreement with Poland which establishes a framework for cooperation between Latvia’s Military Information Technology Security 64 Incident Team (MilCERT) and Poland’s National Cyber Security Center.36 Latvia is also taking the opportunity to reach out to the United States to discuss cybersecurity in the region.37 Lithuania has, as aforementioned, developed their own cyber center the RCDC, which is a bilateral LithuanianUS initiative.38 Conclusion To conclude, the domain of cyberspace will be an arena for battle for the foreseeable future. All countries, governments, militaries will be faced with such threats, and the likelihood of businesses and private individuals being faced with such threats is high. The Baltic states are no strangers to such threats and have been leaders in facing up to them. Given the nature of threats faced and the manner in which the Baltics have faced up to them, it is safe to say that the Baltic states will continue to rise up to the challenges and keep up with the rapidly changing nature of cyber threats. However, the last point is the most persisting challenge any entity faces in cyberspace – the need to not only consistently keep up but remain steps ahead of adversaries. The bi- and multilateral agreements made as well as the leadership demonstrated, and the digital awareness can go a long way to not only meet contemporary and future challenges but serve as examples and demonstrate leadership. Cyber and hybrid threats are ominous, but on a positive note, the Baltic states have achieved many remarkable accomplishments in this field.

#### Taiwan-Lithuania cooperation key to defend against Chinese cyberattacks

Cole 21 (J. Michael Cole, Senior Advisor, Countering Foreign Authoritarian Influence (CFAI) at the International Republican Institute (IRI); Global Taiwan Institute, Macdonald-Laurier Institute, Prospect Foundation. Senior Non-Resident Fellow @ Global Taiwan Institute, Masters in War Studies @ Royal Military College of Canada, International Diploma in Humanitarian Assistance @ Fordham University. “The Lithuanian model for expanding Taiwan’s ties with Baltic States”, https://www.caribbeannewsglobal.com/the-lithuanian-model-for-expanding-taiwans-ties-with-baltic-states/)LR

The establishment of a representative office in Lithuania constitutes a victory for Taiwan in its efforts to counter both international isolation and the Chinese narrative of Taiwan’s supposedly inevitable international isolation. By focusing on a part of the world that has not traditionally been an area for Taiwanese presence and engagement, Taipei has also demonstrated the virtues of an asymmetrical approach to combating China on the world stage. This development also exposes the fact that Beijing is willing to break its own rules on “One China,” in that it is now willing to punish states even when they continue to abide by their “One-China Policy” by not establishing official ties with Taiwan. Although the object of Beijing’s ire is ostensibly related to the nomenclature used for Taiwan’s office in Vilnius (which uses the word “Taiwan”), at a deeper level, the source of its anger is the gains that Taiwan has made in Europe, an area where China had hoped to increase its influence. Lithuania has taken some risks in placing its bets on Taiwan, and besides the retaliation it is currently facing, the move may also have cost it future economic opportunities. Consequently, it will be crucial for Taiwan to demonstrate that Vilnius’ risk-taking was not in vain. Already, a large Taiwanese trade and investment delegation has visited the country, with a total of 240 online and offline trade talks involving more than 150 Lithuanian firms and various Taiwanese ones. Taiwan must build on the complementarity of the two economies to replicate its successes in countries like the Czech Republic, where despite much Chinese propaganda, Taiwan has been a much more substantial investor and job creator. Lithuania has a hard-working, highly educated and productive workforce in the manufacturing sector, with strengths in areas such as the laser industry—which has also become a target for Chinese retaliation, with China deciding to halt cooperation between its laser industry bodies and Lithuania. Trade forms the basis of bilateral relations and must be mutually beneficial. Lithuania has made it clear that it expects to reap the benefits of engagement with Taiwan, a country with an economy approximately 11 times larger than its own, as well as a highly advanced tech sector. Lithuania therefore represents a golden opportunity for Taiwan to showcase the advantages of engagement and to demonstrate that small and medium states not only can afford to defy China but can actually benefit materially from doing so. Conversely, failure to build upon and to sustain this momentum could dissuade prospective partners from going down that path. Thus, Taipei must demonstrate a commitment to building prosperous and mutually beneficial ties with its new Baltic ally, and the tangible results must materialize as expeditiously as possible. The potential for engagement between Taiwan and the Baltics goes well beyond trade and investment, however. Lithuania, Latvia, and Estonia all have traditions of resistance to external aggression and, by virtue of their proximity to Russia, have developed their own strategies to counter the security threat posed by their much more powerful – and like China, expansionist neighbor. Taiwan and the Baltic states, therefore, have much to learn from each other, in areas ranging from cyber and hybrid warfare to the implementation of an asymmetrical defense posture. While Russia poses the more immediate threat to the Baltic region underscored by apprehensions across the region that Moscow could launch an invasion of Ukraine as early as next January – it is also clear that China has become a more active player in the region, with all the risks of espionage, cyberattacks, co-optation, and hybrid threats that this new presence entails. Countries like Lithuania that have already defied Beijing are now bracing for the very real possibility of cyberattacks against their institutions, and this is an area where Taiwan’s expertise in addressing such threats can come in handy. **Appropriate intelligence-sharing mechanisms** must therefore be established to facilitate communication, threat mitigation, and response; these are areas where, again, Baltic states can make real gains from a deeper relationship with Taiwan, whose capabilities in the cyber sector are larger by orders of magnitude. The fledgling relationship with this part of Europe also creates opportunities for Taiwan’s indigenous defense industry, particularly in the unmanned vehicle sector: for example, Taiwan donated 10 police drones to Lithuania in October to assist the country as it deals with an influx of refugees from Belarus. For its part, Taiwan has much to learn from the Baltic states in non-traditional military areas, particularly in areas of state resilience and the concept of total defense. For example, as it explores ways by which to increase its deterrence against a Chinese attack, the Taiwanese military could learn important lessons from the Lithuanian Lietuvos Šaulių Sąjunga (“Riflemen’s Union”), the Estonian Defense League, and the National Guard, initiatives that blend traditional military forces with a militia and civilian component. Among other things, Taiwan could learn from those countries’ experiences in providing training to these additional layers of defense, as well as how and where to safely store weapons so that they can be quickly accessed by paramilitary forces in times of national emergency. No doubt Taiwan could learn a thing or two about forming and training a proper Reserve Force. Taiwan and the Baltics can also identify areas for the joint training of special forces and other units charged with waging asymmetrical war against a much more powerful and better-equipped opponent. Latvia and Lithuania, in particular, have clearly signaled their willingness to engage Taiwan more closely on such matters. For this to happen, the Taiwanese government will have to be willing to go beyond its traditional areas of engagement on security issues, and civilian authorities will have to contend with a culture of historical resistance within the ministry of national defense to the idea of giving the population a role in national security (especially one that involves arming them). But as with trade, Taipei will need to overcome those difficulties and, as rapidly as possible, demonstrate to its potential partners that it is ready to engage them in a way that is mutually beneficial. As the experience with Lithuania shows, an unprecedented window of opportunity has been created for Taiwan in the Baltics -one that will not remain open indefinitely. While we cannot expect results overnight, especially on security matters, Taipei cannot afford to drag its feet – and must therefore be proactive in its efforts to turn this potential into a source of real benefits for all the countries involved. It has natural and willing partners in the Baltics; Taipei, too, must demonstrate that it means what it says. If it does well in that area, there is a high likelihood that countries elsewhere will take notice. Failure to seize this moment, however, could have long-term detrimental effects on Taiwan’s appeal, and thereby strengthen China’s ability to deter engagement with Taiwan. The ball, therefore, is very much in Taipei’s court. The main point: A window of opportunity has opened for Taiwan to deepen its engagement with the Baltic states, a grouping of small nations that also faces an existential threat from a powerful authoritarian neighbor. In areas ranging from trade to non-traditional defense, these states are natural allies for Taiwan, and provide a chance for Taipei to showcase the real benefits of closer ties despite threatened retaliation by Beijing.

#### \*\*\*Chinese cyberattacks destabilize Taiwan

* Cyber - -> invasion and PRC can destabilize/counter US forces

Sacks 22 (David, research fellow at the Council on Foreign Relations, where his work focuses on U.S.-China relations, U.S.-Taiwan relations, Chinese foreign policy, cross-Strait relations, and the political thought of Hans Morgenthau. “Enhancing U.S.-Japan Coordination for a Taiwan Conflict”, https://cdn.cfr.org/sites/default/files/report\_pdf/Enhancing%20U.S.-Japan%20Coordination%20for%20a%20Taiwan%20Conflict\_DP\_1.pdf)LR

Adding to the worry, over the past five years China has steadily increased its pressure on Taiwan, reducing the number of mainland tourists who can visit the island, stripping away its few remaining diplomatic partners, placing an embargo on certain Taiwanese exports, ramping up military activities in its vicinity, conducting cyber-attacks, and interfering in Taiwan s democratic process. While Xi continues to publicly stress his commitment to peaceful reunification” with Taiwan and has not introduced an explicit timeline for achieving this objective, he has also said that the Taiwan issue cannot be passed on from generation to generation.”2 He has set 2049 as the date by which China must achieve the great rejuvenation of the Chinese nation,” and achieving reunification” with Taiwan is a core condition for that project.3 Still, it remains unlikely that Xi has already decided to use force against Taiwan, which provides an opening for the United States to adjust its policies and work with its allies to help prevent such an outcome. Although there is debate over whether China will resort to force, China is clearly developing capabilities needed to invade and occupy Taiwan. Preparing for a conflict over Taiwan has driven China s military modernization campaign for the past two and a half decades. China has invested significant resources in developing the tools to defeat Taiwan and prevent the United States from coming to its aid, principally an arsenal of accurate ballistic missiles, the world’s largest navy, hundreds of modern fighter aircraft and bombers, and advanced cyber and counterspace assets The recommendations proposed, while ambitious, are feasible in the current political climate in both Washington and Tokyo, and, with sustained focus in both capitals, can be implemented in the next five years. While China has a number of options it could take to put pressure on Taiwan—seizing an offshore island, initiating massive cyberattacks, firing hundreds of ballistic missiles to take out critical infrastructure, and conducting a quarantine of the island—this paper focuses squarely on how to deter and respond to an invasion of Taiwan. It does so in the belief that Japan s appetite for assisting the United States in countering Chinese aggression against Taiwan short of a full war is politically challenging and likely limited. China is not relying on its inherent advantages, however, and has instead spent the last two and a half decades developing capabilities designed to neutralize U.S. power in the Taiwan Strait. Its military budget has grown from $14.3 billion in 1996 to $252.3 billion in 2020, a nearly eighteenfold increase (see figure 2).7 Preparing for a conflict over Taiwan has consistently driven Beijing s procurement decisions, and China can now bring significant capabilities to bear. The PLA Navy (PLAN) is now the largest navy in the world (as measured by the number of ships, although the United States continues to exceed it by tonnage), with 355 ships and submarines, and is set to grow by nearly 100 ships by the end of the decade.8 The PLA Air Force is the largest air force in the region and is rapidly catching up to Western air forces” and eroding U.S. advantages, according to the U.S. Department of Defense.9 The PLA has one thousand short-range ballistic missiles and six hundred medium-range ballistic missiles in its arsenal.10 China has also established an advanced integrated air defense system on its east coast that can cover Taiwan.11 The PLA is now turning its attention to addressing previous gaps that have persisted, such as anti-submarine warfare, while also rapidly developing information, cyber, and space and counterspace capabilities.12 Taiwan, however, is belatedly recognizing the need to dramatically rethink and invest in its defense. In 2017, its military leadership introduced the Overall Defense Concept(ODC), which aims to develop asymmetric approaches to fend off a Chinese invasion and calls for investing in a large number of smaller, cheaper, and more mobile weapons.23 Rather than seeking to defeat the PLA through attrition, ODC focuses on a decisive fight near Taiwans shores and the prevention of a successful PLA landing. Taiwan has steadily increased its defense budget in recent years, which is now the highest it has ever been in absolute terms.24 More important is using these funds to resource an asymmetric strategy, purchasing missiles, drones, and howitzers.25 There remain obstacles to ODC s implementation, however, and more traditional thinking could well make a comeback.26 All of this means that U.S. intervention on Taiwan s behalf would be a risky and costly proposition, as China can now challenge the United States across all domains and place U.S. aircraft, surface vessels (including aircraft carriers), and bases throughout the Indo-Pacific at risk. In addition, the United States would for the first time be fighting a nuclear-armed opponent with precision standoff weapons, extensive cyberwarfare capabilities, and the ability to target its satellites.27

#### China-Taiwan war goes nuclear. Deterrence is key.

Pettyjohn and Wasser 5-20-2022, \*senior fellow and director of the defense program at the Center for a New American Security, \*\*fellow in the defense program and co-lead of The Gaming Lab at the Center for a New American Security (Stacie and Becca, “A Fight Over Taiwan Could Go Nuclear,” *Foreign Affairs*, <https://www.foreignaffairs.com/articles/china/2022-05-20/fight-over-taiwan-could-go-nuclear/)//BB>

Russia’s invasion of Ukraine has raised the specter of nuclear war, as Russian President Vladimir Putin has placed his nuclear forces at an elevated state of alert and has warned that any effort by outside parties to interfere in the war would result in “consequences you have never seen.” Such saber-rattling has understandably made headlines and drawn notice in Washington. But if China attempted to forcibly invade Taiwan and the United States came to Taipei’s aid, the threat of escalation could outstrip even the current nerve-wracking situation in Europe. A recent war game, conducted by the Center for a New American Security in conjunction with the NBC program “Meet the Press,” demonstrated just how quickly such a conflict could escalate. The game posited a fictional crisis set in 2027, with the aim of examining how the United States and China might act under a certain set of conditions. The game demonstrated that China’s military modernization and expansion of its nuclear arsenal—not to mention the importance Beijing places on unification with Taiwan—mean that, in the real world, a fight between China and the United States could very well go nuclear. Beijing views Taiwan as a breakaway republic. If the Chinese Communist Party decides to invade the island, its leaders may not be able to accept failure without seriously harming the regime’s legitimacy. Thus, the CCP might be willing to take significant risks to ensure that the conflict ends on terms that it finds acceptable. That would mean convincing the United States and its allies that the costs of defending Taiwan are so high that it is not worth contesting the invasion. While China has several ways to achieve that goal, from Beijing’s perspective, using nuclear weapons may be the most effective means to keep the United States out of the conflict. China is several decades into transforming its People’s Liberation Army (PLA) into what the Chinese President Xi Jinping has called a “world-class military” that could defeat any third party that comes to Taiwan’s defense. China’s warfighting strategy, known as “anti-access/area denial,” rests on being able to project conventional military power out several thousand miles in order to prevent the American military, in particular, from effectively countering a Chinese attack on Taiwan. Meanwhile, a growing nuclear arsenal provides Beijing with coercive leverage as well as potentially new warfighting capabilities, which could increase the risks of war and escalation. China has historically possessed only a few hundred ground-based nuclear weapons. But last year, nuclear scholars at the James Martin Center for Nonproliferation Studies and the Federation of American Scientists identified three missile silo fields under construction in the Xinjiang region. The Financial Times reported that China might have carried out tests of hypersonic gliders as a part of an orbital bombardment system that could evade missile defenses and deliver nuclear weapons to targets in the continental United States. The U.S. Department of Defense projects that by 2030, China will have around 1,000 deliverable warheads—more than triple the number it currently possesses. Based on these projections, Chinese leaders may believe that as early as five years from now the PLA will have made enough conventional and nuclear gains that it could fight and win a war to unify with Taiwan. Our recent war game—in which members of Congress, former government officials, and subject matter experts assumed the roles of senior national security decision makers in China and the United States—illustrated that a U.S.-Chinese war could escalate quickly. For one thing, it showed that both countries would face operational incentives to strike military forces on the other’s territory. In the game, such strikes were intended to be calibrated to avoid escalation; both sides tried to walk a fine line by attacking only military targets. But such attacks crossed red lines for both countries, and produced a tit-for-tat cycle of attacks that broadened the scope and intensity of the conflict. For instance, in the simulation, China launched a preemptive attack against key U.S. bases in the Indo-Pacific region. The attacks targeted Guam, in particular, because it is a forward operating base critical to U.S. military operations in Asia, and because since it is a territory, and not a U.S. state, the Chinese team viewed striking it as less escalatory than attacking other possible targets. In response, the United States targeted Chinese military ships in ports and surrounding facilities, but refrained from other attacks on the Chinese mainland. Nevertheless, both sides perceived these strikes as attacks on their home territory, crossing an important threshold. Instead of mirror-imaging their own concerns about attacks on their territory, each side justified the initial blows as military necessities that were limited in nature and would be seen by the other as such. Responses to the initial strikes only escalated things further as the U.S. team responded to China’s moves by hitting targets in mainland China, and the Chinese team responded to Washington’s strikes by attacking sites in Hawaii. A NEW ERA One particularly alarming finding from the war game is that China found it necessary to threaten to go nuclear from the start in order to ward off outside support for Taiwan. This threat was repeated throughout the game, particularly after mainland China had been attacked. At times, efforts to erode Washington’s will so that it would back down from the fight received greater attention by the China team than the invasion of Taiwan itself. But China had difficulty convincing the United States that its nuclear threats were credible. In real life, China’s significant and recent changes to its nuclear posture and readiness may impact other nations’ views, as its nuclear threats may not be viewed as credible given its stated doctrine of no first use, its smaller but burgeoning nuclear arsenal, and lack of experience making nuclear threats. This may push China to preemptively detonate a nuclear weapon to reinforce the credibility of its warning. China might also resort to a demonstration of its nuclear might because of constraints on its long-range conventional strike capabilities. Five years from now, the PLA still will have a very limited ability to launch conventional attacks beyond locations in the “second island chain” in the Pacific; namely, Guam and Palau. Unable to strike the U.S. homeland with conventional weapons, China would struggle to impose costs on the American people. Up until a certain point in the game, the U.S. team felt its larger nuclear arsenal was sufficient to deter escalation and did not fully appreciate the seriousness of China’s threats. As a result, China felt it needed to escalate significantly to send a message that the U.S. homeland could be at risk if Washington did not back down. Despite China’s stated “no-first use” nuclear policy, the war game resulted in Beijing detonating a nuclear weapon off the coast of Hawaii as a demonstration. The attack caused relatively little destruction, as the electromagnetic pulse only damaged the electronics of ships in the immediate vicinity but did not directly impact the U.S. state. The war game ended before the U.S. team could respond, but it is likely that the first use of a nuclear weapon since World War II would have provoked a response. The most likely paths to nuclear escalation in a fight between the United States and China are different from those that were most likely during the Cold War. The Soviet Union and the United States feared a massive, bolt-from-the-blue nuclear attack, which would precipitate a full-scale strategic exchange. In a confrontation over Taiwan, however, Beijing could employ nuclear weapons in a more limited way to signal resolve or to improve its chances of winning on the battlefield. It is unclear how a war would proceed after that kind of limited nuclear use and whether the United States could de-escalate the situation while still achieving its objectives. AN OUNCE OF PREVENTION The clear lesson from the war game is that the United States needs to strengthen its conventional capabilities in the Indo-Pacific to ensure that China never views an invasion of Taiwan as a prudent tactical move. To do so, the United States will need to commit to maintaining its conventional military superiority by expanding its stockpiles of long-range munitions and investing in undersea capabilities. Washington must also be able to conduct offensive operations inside the first and second island chains even while under attack. This will require access to new bases to distribute U.S. forces, enhance their survivability, and ensure that they can effectively defend Taiwan in the face of China’s attacks. Moreover, the United States needs to develop an integrated network of partners willing to contribute to Taiwan’s defense. Allies are an asymmetric advantage: the United States has them, and China does not. The United States should deepen strategic and operational planning with key partners to send a strong signal of resolve to China. As part of these planning efforts, the United States and its allies will need to develop war-winning military strategies that do not cross Chinese red-lines. The game highlighted just how difficult this task may be; what it did not highlight is the complexity of developing military strategies that integrate the strategic objectives and military capacities of multiple nations. Moving forward, military planners in the United States and in Washington’s allies and partners must grapple with the fact that, in a conflict over Taiwan, China would consider all conventional and nuclear options to be on the table. And the United States is running out of time to strengthen deterrence and keep China from believing an invasion of Taiwan could be successful. The biggest risk is that Washington and its friends choose not to seize the moment and act: a year or two from now, it might already be too late.

## Potential Plan

#### The United States federal government should substantially increase its cyber security cooperation with the North Atlantic Treaty Organization in cyber security in Latvia, Lithuania, and Estonia through shared cooperation of cyber defense

## Solvency

#### The plan models NATO cybersecurity after the Baltics – empirically dissuades Russian attacks and secures US infrastructure.

Atalayar 7-20 [Atalayar, 7-20-2022, "The Baltic States, a defence model for the future of cyberwarfare", https://atalayar.com/en/content/baltic-states-defence-model-future-cyberwarfare, DOA: 7-20-2022 //ArchanSen]

The world is moving towards a digitised global society full of cyber opportunities. However, as a fully cyber-connected society, this future society will also have to cope with new patterns of conflict, such as cyber-attacks and hybrid warfare.

The Baltic countries - Estonia, Latvia, and Lithuania - which for years were under the control of the Union of Soviet Socialist Republics (USSR) and then forced to fight on the front line of digital warfare, have been forced to take the lead in this process of cyber-innovation. Moscow's attacks on the three pioneers of independence from the USSR have been a constant for years. And they have grown exponentially since the early 2000s.

The Estonian example

The Republic of Estonia was one of the Kremlin's first targets in 2007. Tallinn's decision to move the monument to the fallen Soviet soldiers of World War II from the centre of the capital to the 'Bronze Soldier' cemetery provoked a wave of cyber-attacks from Russia that lasted more than 20 days. Public and private organisations, ministries, banks, the media and even the parliament itself were affected by hundreds of hacker offensives.

"The government website normally receives between 1,000 and 1,500 hits a day; at the height of the attacks, in the first week of May, it received between 1,000 and 1,500 per second," explained defence spokesman Mikko Maddis at the time. "It blew up the system.”

Fearing that the attack was just the prelude to a larger-scale cyber offensive, Estonia armoured itself. The small country shifted as many government services and systems as possible to new, private and secure networks, improving cyber security and protecting itself against the effects of digital warfare. This path also led Tallinn to transfer citizen services and the most basic government functions to blockchain technology.

Today, Estonia has become a country capable of dealing with almost any cyber threat; defined by The New Yorker as a "digital republic", its citizens have the opportunity to access virtually all available government services online, and its political and economic leaders to run it effectively from anywhere in the world.

Indeed, in 2014 Tallinn spearheaded the world's first e-residency programme, aiming to exceed 10 million residents by 2025. And while it has so far failed to add more than 85,000 residents, it has enabled more than 19,000 entrepreneurs to consolidate new digital companies that do not need to be physically present.

#### Cooperation with Estonia is key – promotes cybersecurity for all of NATO

David Shedd 20, professor at the Patrick Henry College, former acting director of the Defense Intelligence Agency; and Ivana Stradner, Visiting Research Fellow at the American Enterprise Institute, J.S.D. from the University of California, Berkeley,8/11/2020, "Countering Russia’s Influence Operations in the Balkans," https://www.heritage.org/europe/commentary/countering-russias-influence-operations-the-balkans, RMax

Even the pandemic has the potential for fomenting political unrest.

In recent days, thousands of Serbs have taken to the streets to protest Serbian President Aleksandar Vucic’s announced strict curfew in response to a surge in Covid-19 cases. Many have pointed a finger at pro-Russia ultra-right groups and foreign intelligence services for fueling the violent riots.

Moscow denies any “Russian trace” in the unrest. Whether Russia is behind the violent protests in Belgrade remains to be seen. One thing is for certain. The Kremlin’s efforts to sow mayhem in the Balkans would not be new; this would merely be the latest attempt by a resurgent Russia to threaten Euro-Atlantic security and challenge the United States’ ability to defend its interests in Europe.

Russia is promoting its interests in the Western Balkans through the widespread use of disinformation and cyberwarfare. The U.S., however, isn’t helpless. It has an opportunity to obtain insights into these efforts and counter Russia's influence campaigns. It is time to confront Russia's strongman Vladimir Putin's cyber games before American interests are permanently damaged in the Balkans.

The U.S. and the E.U. have long been ambivalent about defining their interests in the Western Balkans. Russia has capitalized on these years of neglect and leveraged a power vacuum in the former Yugoslavia to gain economic and political influence. The region is now at the forefront of Russia's use of low-cost strategies to expand its global influence and undermine western interests.

Russian disinformation, aided by repeated cyberattacks on government institutions, was instrumental in the 2016 Moscow-sponsored coup attempt in Montenegro. In North Macedonia, Russia spread disinformation prior to the name-change referendum that finally enabled North Macedonia to join NATO. It also established hundreds of North Macedonia-based “troll factories," from which Russia pedaled fake news against the 2016 U.S. elections. Facebook recently banned troll farms from North Macedonia that pushed COVID-19 disinformation.

Moscow has also been investing in critical sectors in Croatia. With its strategy of fomenting political divisions, the Kremlin has been exploiting internal conflicts in Albania. In Bosnia and Herzegovina, disinformation campaigns have sown ethnic and religious discord, while promoting the secession of ethnic Serb regions from Bosnia. In response, the U.S. should encourage the transatlantic integration for Bosnia and Herzegovina, the Western Balkans’ most fragile country.

Russia has used state-sponsored media to promote nationalist and anti-Western narratives in Serbia, including the opening of a Sputnik office in Belgrade. Also,  Russian-run “Humanitarian Center” in Serbia is very close to the main NATO based in Kosovo (Camp Bondsteel). Some European and American officials fear that it serves as a base for the Kremlin intelligence-gathering activities to eavesdrop on U.S. interests in the Balkans.

Russia’s preeminent goals in the Balkans have been to refine their disinformation tactics and erode Western influence in the region, including in Croatia, Montenegro, North Macedonia and Albania, which are all NATO members. The West needs to aggressively respond to this Russian posture, including using a cyber-focused campaign to counter Russia's provocations.

For crafting such a strategy, the West should look to Estonia. After the 2007 Russian cyberattack on Estonian government institutions, Estonia became a global leader in cybersecurity and home to the NATO Cooperative Cyber Defense Centre of Excellence, which is a cyber-defense hub that supports member nations with cyber-defense expertise. A similar approach by the West would benefit the Western Balkans, where information and communication technology sector is the most promising and the fastest growing economic sector in the region. In Serbia alone, the I.T. sector generates more than 10% of GDP with a similar trend in other countries in the region, which have some of the highest numbers of outsourced I.T. workers per capita in Europe.

An American-led strategy should focus on creating a regional cyber-security infrastructure in the Western Balkans, modeled on Estonia's example. Given that countries in the Western Balkans share the same cyber-security threats from Russia and, more recently, from China, a regional hub for cybersecurity would allow states to cooperate among each other in cyber deterrence, attribution of attacks and collective countermeasures.

Several countries in the Western Balkans have joined NATO, but alliances are notoriously unreliable, especially among the smaller states. Countries in the Western Balkans need strong NATO and E.U. ties to withstand Russian influence. Cyber-security is one of the areas where they can strengthen their positions in allegiance with the western democracies.

The timing is excellent for the U.S. to establish a regional cyber-security hub in the Western Balkans. Immediate steps need to be taken to halt malign Russian influence. With elections approaching this year in the U.S., North Macedonia, Croatia and Montenegro, countries should continue cooperating to counter malicious Russian cyber activities.

The U.S. can learn more about Russian cyber tactics at the same time. One way to send a strong message would be to deploy a cyber-team to strengthen NATO’s countries’ cyber-capabilities in an effort to thwart future Russian network intrusions such as the one that was undertaken by Russian intelligence operators in Bulgaria in 2017.

Serbia, a key ally to Moscow in the region, remains the biggest obstacle to countering Russian influence. Serbia just had parliamentary elections boycotted by the opposition that resulted in Vucic's Serbian Progressive party winning a landslide victory and further strengthening his power. The close Russia-Serbian relationship can make it difficult to detect Russia's subversive activities.

Of all the Western Balkans countries, Serbia had the highest military expenditure in 2019, and President Vucic thanked Russia for making Serbia’s military 10 times stronger since NATO intervention in 1999. After Russia employed an S-400 missile system in Serbia for a military drill, the Pantsir S1 air-defense systems were delivered this past February, despite a looming U.S. sanctions threat.

Should Serbia continue obtaining Russian weapons, Washington should impose sanctions. Serbia must understand that its strategy of neutrality is unacceptable to the U.S., as are its claims to balance their interests among Russia, China and the West. The U.S. should remain solidly committed, leading efforts to solve the Kosovo dispute and wrest control of that narrative from Russia.

While variances in the national interests may complicate cooperation among the Western Balkan countries, they share similar vital objectives that make cooperation possible and even attractive under U.S. leadership. Among these are the historical fear of Russian domination and a desire for E.U. and NATO membership. A U.S.-led strategy with NATO country participation to enhance their cyber-capabilities will improve their security in countering nefarious Russian influence while enhancing cooperation between Balkan nations.

Moscow is determined to expand its influence in the Western Balkans, using cyber-warfare at the expense of U.S. and western interests. To prevent it, the U.S. should design a new strategy for the Western Balkans that demonstrates that the U.S. is committed to countering Russia's disruptive activities in the Western Balkans and beyond. The time for that response is now.

#### Estonia especially good at countering disinfo

* Cyberattacks in general too

Pernik 21 (Piret, is a researcher at the NATO Cooperative Cyber Defence Centre of Excellence (CCDCOE). She has researched cybersecurity strategic and policy aspects since 2013. She has published research reports and analyses on cyber resilience, military 5G security, cyber commands, and cyber defence training. She is also a co-editor of the volume Cyber Threats and NATO 2030: Horizon Scanning and Analysis, published by the CCDCOE. Her articles have been published in academic journals and she has written book chapters, as well as online commentaries. She holds an MA in Social Sciences from the University of Tallinn, and an MA in International Relations and European Studies from the Central European University, Budapest. “Cyber deterrence: A case study on Estonia’s policies and practice”, https://www.hybridcoe.fi/wp-content/uploads/2021/10/20211012\_Hybrid\_CoE\_Paper\_8\_Cyber\_deterrence\_WEB.pdf)LR

Estonia does not have a standalone policy of cyber deterrence, but strategic documents relating to national security, foreign policy and cybersecurity describe diverse components of cyber deterrence. Cybersecurity is deemed a part of foreign, security and defence policy, as well as domestic/internal security. It is also included in strategic documents and policies concerning digital modernization, technology, education and research, and so forth. The review and analysis of Estonia’s strategic documents associated with cybersecurity (presented in Annex I) shows that two concepts – cross-domain deterrence and cyber deterrence – play an important role in the government’s cybersecurity discourse. Three layers of deterrence – entanglement and norms, denial and punishment – are equally upheld. Generally speaking, the analysis demonstrates that in the Estonian national security discourse, deterrence by denial and punishment tend to be conceptualized in the context of national security and defence policy; entanglement and norms in the context of foreign policy and cyber diplomacy; and denial (domestic defence/resilience) in the context of digital and technology policies. In the latest strategy (2019–2022), cyber deterrence is referenced almost as frequently as in the 2014–2017 document, apart from the fact that cross-domain deterrence and military deterrence are not mentioned. Rather, concerns about challenges relating to digital modernization and technology policies come to the fore in this strategy. The last column of Table 2 provides examples of how a deterrence tool has been implemented. Table

Description automatically generated To strengthen its cyber diplomacy capacity, Estonia established a position in 2018 for an ambassador-at-large for cybersecurity. Estonia is one of the leaders among the Baltic and Nordic countries when it comes to cyber diplomacy. It has been a member of the UN Group of Governmental Experts for many years, and is also a leader in cyber diplomacy education for foreign diplomats.35 As a member of the UN Security Council in 2020– 2021, in June 2021 Estonia organized for the first time in the Council’s history an open meeting on cybersecurity, where it raised the issue of state behaviour in cyberspace in the context of international peace and security.36 Since 2008, Estonia has hosted the NATO Cooperative Cyber Defence Centre of Excellence (CCDCOE), which sponsors the publication of world-renowned scholarly works on international law applicable to cyberspace – the Tallinn Manuals 1.0 (2013), 2.0 (2017), and the forthcoming volume 3.0.37 Deterrence by denial, conceptualized in Estonia primarily as domestic defence/resilience measures, is foundational for the country’s cybersecurity posture.38 Deterrence in this area includes a full spectrum of activities prescribed in the national cybersecurity strategies, in cybersecurity legislation and other relevant ministerial regulations. Some of the resilience-related objectives have remained constant since 2008, such as applying measures to harden networks (for example, standards, risk analysis and management tools, incident response, raising awareness, building cybersecurity capacity and competence, to name a few).39 In June 2021, Estonia published its first national information security standard entitled E-ITS, which is a guideline for public and private network owners and operators to ensure minimum security standards.40 The Estonian Information System Authority regularly alerts stakeholders and the general public to cyber threats, vulnerabilities and exploits, and helps them to protect their networks. These activities contribute to deterrence by denial by increasing the ability to protect networks and recover from cyber incidents. Public attribution can be regarded as a tool for deterrence.46 Indeed, among Estonian experts, public attribution is regarded as a primary tool of cyber deterrence.47 As noted by scholars, one aim of public attribution is the act of norm-setting – that is, establishing “the rules of the road” and subsequently enforcing appropriate behaviour in cyberspace (response measures).48 In a similar manner, the Estonian government holds that “public statements on attribution can be made, with the aim of increasing accountability in cyberspace and emphasising the importance of adhering to international law obligations and norms of responsible state behaviour”.49 The Estonian Ministry of Foreign Affairs subscribes to the opinion that “public attribution […] allows states to send clear messages and shape expectations that malicious cyberspace operations will not be tolerated” and “it is necessary to send a message that harmful cyberspace operations are not part of acceptable state behaviour”.50 In other words, Estonia directly links public attribution to setting cyber norms, thus connecting deterrence by entanglement and norms to legal consequences, namely deterrence by punishment. According to this view, Estonia supports public attribution and collective measures “where possible” and “public attribution and messaging are tools for deterring and responding […] but also for raising wider awareness”.51 To support collective public attribution and to hold violators responsible, Estonia actively contributes to EU and NATO cyber deterrence discussions, and belongs to the US-led international cyber deterrence initiative.52 Based on the Estonian case study, a policy recommendation for EU and NATO countries is to apply a three-layered deterrence model.73 First, EU and NATO countries should participate in entanglement and norms measures such as cyber diplomacy and capacity-building globally. Second, they should invest more in denial measures and, third, jointly develop policies for punitive response options, including developing public attribution procedures to enable quick attribution, and systematically implementing sanctions regimes. It would be feasible to establish memoranda of understanding, and operational- and technical-level frameworks to radically improve information- and intelligence-sharing. Participation in cyber defence and crisis management exercises should be open to like-minded NATO partner countries. Joint bilateral cyberspace operations likewise contribute to mutual trust-building and information-sharing, and increase parties’ operational and technical competence.74 Operational- and technical-level joint activities should be regularly practised among allies and with like-minded partners as they contribute to deterrence by denial. Given that NATO’s cyber With regard to deterrence by denial, Estonia, together with other EU and NATO countries, should develop a zero trust security strategy and architecture.75 Zero trust is a cybersecurity paradigm that treats networks as untrusted, and that moves defences from static, network-based perimeters to focus on users, assets, and resources. It assumes that there is no implicit trust granted to user accounts or assets in any network segment (including a corporate local area network), and applies authentication and authorization before a session is established.76 While deterrence might work at the high end, novel security principles should be implemented by governments because deterrence is not sufficient to deter cyberattacks. Estonia’s public attribution guidelines serve as a blueprint for other countries to attribute cyberattacks and impose meaningful costs. A sharper focus on responses to high- and low-end cyberattacks should be developed in the future along with concrete deterrence actions and tools for individual 75 For example, the US government has released a strategy, architecture and maturity model that the US federal government agencies will implement: ‘Moving the U.S. Government Towards Zero Trust Cybersecurity Principles’, The White House, https://zerotrust.cyber.gov/. 76 Scott Rose, Oliver Borchert, Stu Mitchell and Sean Connelly, ‘Zero Trust Architecture SP 800-207’, August 2020, NIST, https://csrc.nist.gov/publications/detail/sp/800-207/final. 77 ‘Nye, Deterrence and Dissuasion in Cyberspace’, p. 62. sectors and target types. For example, deterrence tools can differ for diverse targets: internet voting and e-health systems would be targeted by different cyber threat actors that have political or criminal motives, and the same tool is not effective across all actors. Estonia’s forms of cyber deterrence are not effective individually, nor every time, but when implemented together in a whole-of-society approach, and systematically over a longer period of time, it is likely that many malicious cyberattacks can be deterred. As Joseph Nye pointed out, deterrence tools “can complement one other in affecting actors’ perceptions of the costs and benefits of particular actions”.77 Certainly, one cannot deter all cyberattacks – especially those conducted as part of malicious influencing campaigns below the threshold of the use of force – however, it is possible to reduce the number and effect of strategic cyberspace operations. It is likely that punitive responses may deter hostile actors from conducting similar attacks in the future. It will remain to be seen whether the EU and NATO can deter cyberattacks both above and below the threshold of an armed attack better in the future when they apply systematically stronger punitive responses.

#### Mutual Cooperation is key

Horchakova 2022, Veronika Horchakova Mykolas Romeris University, European and International Business Law program, Master’s degree student(“STRENGTHENING THE TRANSATLANTIC PARTNERSHIP: CHALLENGES AND OPPORTUNITIES FOR THE BALTIC STATES” https://repository.mruni.eu/bitstream/handle/007/18311/Teisines\_minties\_svente-97-107.pdf?sequence=1)

In conclusion, taking into account the current geopolitical situation and the number of commitments in the international arena, the Baltic States are likely to remain strong US allies and important US security partners in Europe. Analysts believe that close cooperation between the United States and the Baltic States will continue for the foreseeable future in areas such as efforts to deter potential Russian aggression, the future of NATO, energy security, and socioeconomic issues. As long as there are objective fears of peace demolition, NATO is interested in deepening cooperation with like-minded countries. There is still work to be done within the Baltic region to strengthen resistance to Russian propaganda and maintain sovereignty and determination towards pro-European standards in the socio-economic field. This work will follow, for instance, the example of banning Russian propaganda in the media. To achieve this, the Baltic States will likely continue to rely on the United States for leadership on foreign policy and security issues. This can be seen from current partnership programs devoted to enhancing defence power and providing training and an educational practicum. This reliance is not only from the side of the Baltic region; it is seen as a reciprocal one. For instance, there are climate change issues where Lithuania can share its experience and the best approaches to green ecology with the United States, and the US may be more eager to cooperate with Lithuania. Moreover, in terms of geopolitics, the United States should try to defeat China’s attempts to collaborate with US allies on the same issues. On successfully implementing and finalising those partnership activities, further steps will be taken to proceed with cooperation. In short, the United States’ commitment to Baltic security is part of the US commitment to European security, and the former would not and cannot exist without the latter. As new challenges are emerging, more efforts should be made to guarantee these commitments, thus strengthening transatlantic ties concerns building this partnership, reinforcing power, and preventing threats. This attitude undoubtedly appears to be beneficial for both sides.

# Cyber Advantage Cards

## Attacks coming now

#### Attacks are coming to the Baltics, Ukraine was the brink

* Retag
  + for spillover across the rest of Europe
  + Estonia and Lithuania helping against cyberattacks, they have the expertise

Cerulus 2-22 (Laurens Cerulus leads POLITICO Europe’s team of reporters covering cybersecurity, privacy and data protection issues as Cybersecurity Editor. He also supports the broader team of reporters covering technology issues as Deputy Technology Editor. He is a graduate of City University London’s journalism department and holds master’s degrees in history and international politics. He is a Belgian, born in Leuven. “Cyber ‘spillover’ from Ukraine looms in the Baltics” <https://www.politico.eu/article/baltic-cyber-spillover-ukraine-russia-attack/)LR>

The conflict between Russia and Ukraine puts neighboring EU countries at risk of disruption from cyberattacks and the spread of disinformation, officials warned Tuesday. "The Baltic states, for Russia, are the easiest way to put pressure on the EU and NATO ... This is the place where **we have to pay careful attention**," said Bart Groothuis, Liberal member of the European Parliament and former cybersecurity official at the Dutch Ministry of Defense. Groothuis is leading a delegation of members of the European Parliament's subcommittee on defense and security on visits to Estonia on Tuesday and Lithuania on Wednesday, in what he said was a "show of solidarity" with Ukraine. Those two Baltic countries are already involved in a cyber defense operation to support Ukraine through the EU's Cyber Rapid Response Team, which was activated Tuesday. The threat of cyberattacks on European soil is two-fold: First, attacks launched on Ukrainian networks could spread to European networks. Second, Russia could choose to launch direct attacks on European targets through its intelligence services or cybercriminal groups to disrupt the West's response to the Ukraine crisis. Cyberattacks on Ukraine have affected Europe in the past. In 2017, hackers spread malware known as NotPetya through a Ukrainian piece of software and triggered a worldwide cyber crisis seen as the most devastating cyberattack in history. Western security services later attributed the attack to Russia's military intelligence agency GRU. "There is always the threat of a spillover" like NotPetya, said Jaak Tarien, director at the Cooperative Cyber Defence Centre of Excellence (CCDCOE), a NATO-accredited cyber defense center based in Tallinn that advises the defense alliance and its members on cybersecurity. "It's the one internet we're using," Tarien said, pointing to the connections Europe's tech networks have with Ukraine. Baltic countries, in particular, in past years were often the target of campaigns by Russian state-backed hacking groups targeting public and private institutions. The EU attributed a campaign known as "Ghostwriter" at least in part to Russia, after it first plagued Baltic countries with phishing emails and disinformation campaigns and then moved on to target Polish and German politicians. Countries like Estonia and Lithuania have also emerged as vocal proponents of a tougher response to Russian cyber aggression in Europe. Officials in the Baltics are now on high alert, expecting more attacks to come from Russia as the conflict in Ukraine escalates. Last week, Lithuania's Ministry of Defense raised the alarm, saying it expected serious cyberattacks on the country's public authorities. "We definitely see how, as the general state of security deteriorates, the likelihood of cyber activities increases. We're working on a higher alert level," said Margiris Abukevičius, vice minister at the Ministry of National Defense in Lithuania.

#### Russia perceives the Baltics to not trigger A5.

Heinrichs 22 [Rebeccah L Heinrichs and Timothy Walton., 7-8-2022, "NATO Must Back Lithuania Against Russian Coercion", No Publication, https://rusi.org/explore-our-research/publications/commentary/nato-must-back-lithuania-against-russian-coercion/, DOA: 7-18-2022 //ArchanSen]

Within this context, deterrence could falter in some scenarios. There is a plausible – if still small – chance that Russia could notice US risk-aversion over enabling Ukraine to fight back too hard, and flagging Western support for Ukraine generally, and conclude that attacking a small NATO country would not result in a war with the US. Some may incredulously respond that such an outcome is impossible, because of course the US has the resolve to defend every inch of NATO. Even if the US has such resolve, for deterrence to hold, Moscow must believe that. Deterrence can fail if an aggressor decides that a defending country cannot or will not make good on its deterrent threats. Therefore, strong signals underscoring the US and broader NATO commitment to defend the Baltic states are in order, especially considering Germany’s denunciation of Lithuania’s sovereign decision to enforce EU sanctions on Russia.

#### Baltics invasion coming now.

Thibault Spirlet 22 [Thibault Spirlet, 7-17-2022, "'Is NATO going to fight?' Baltic States on brink of Putin's invasion as EU could cave in", Express.co.uk, https://www.express.co.uk/news/world/1641537/putin-russia-ukraine-war-news-nato-eu-nord-stream-1-sanctions-energy-vn, DOA: 7-18-2022 //ArchanSen]

NATO and the European Union might not get directly involved in a military confrontation with Russia, should Vladimir Putin decide to expand the conflict beyond Ukraine's borders, a former US Ambassador to Ukraine has warned. As Europe is suffering from the economic sanctions imposed on Russia with inflation propelling up prices across the continent, former Ambassador Herbst says it is becoming more likely Europe will cave in. The latest Russian threat is an energy blackmail through the Nord Stream 1 pipeline – currently closed because of maintenance – which may not reopen on the July 21 deadline, dropping Russian gas imports to close to zero – a scenario that could plunge the EU into an energy crisis.

When asked about the possibility of Putin expanding the war beyond Ukraine’s border, Ambassador Herbst told Express.co.uk: "He [Putin] has said he believes he should have a substantial influence in all the post-Soviet countries.

"He has demanded that he can impose restrictions on NATO deployments among the former member of the Warsaw Pact. He’s not hiding this."

On the danger of Russia invading NATO countries, Ambassador Herbst said: "You’ve just described the scenario as plausible where the EU is going to cave to Russia as it is committing mass atrocities in Ukraine.

"So, if the EU is willing to cave on Ukraine, why wouldn’t he bet on the Baltic States – these hard-to-defend little states that have joined the EU only relatively recently and joined NATO relatively recently and that Russia controlled for centuries?"

When pressed on the fact Russia would lose a war against NATO, Ambassador Herbst said: "Why would he assume NATO is going to fight? You’re describing a Europe that is craven – the same European countries that make up the EU make up NATO."

Further elaborating, he said: "I’m saying that Putin might reckon that just as NATO has limited its support to Ukraine, just as the EU caved on sanctions, there will not be enough guts in Europe to defend the Baltic States.

"That is a very plausible scenario.

"What I just said is not a secret. It’s out there in the public domain. But a lot of Europeans refuse to think about this because they live in a dream world."

#### Attacks are coming to the Baltics, Ukraine was the brink

* Retag
  + for spillover across the rest of Europe
  + Estonia and Lithuania helping against cyberattacks, they have the expertise

Cerulus 2-22 (Laurens Cerulus leads POLITICO Europe’s team of reporters covering cybersecurity, privacy and data protection issues as Cybersecurity Editor. He also supports the broader team of reporters covering technology issues as Deputy Technology Editor. He is a graduate of City University London’s journalism department and holds master’s degrees in history and international politics. He is a Belgian, born in Leuven. “Cyber ‘spillover’ from Ukraine looms in the Baltics” <https://www.politico.eu/article/baltic-cyber-spillover-ukraine-russia-attack/)LR>

The conflict between Russia and Ukraine puts neighboring EU countries at risk of disruption from cyberattacks and the spread of disinformation, officials warned Tuesday. "The Baltic states, for Russia, are the easiest way to put pressure on the EU and NATO ... This is the place where **we have to pay careful attention**," said Bart Groothuis, Liberal member of the European Parliament and former cybersecurity official at the Dutch Ministry of Defense. Groothuis is leading a delegation of members of the European Parliament's subcommittee on defense and security on visits to Estonia on Tuesday and Lithuania on Wednesday, in what he said was a "show of solidarity" with Ukraine. Those two Baltic countries are already involved in a cyber defense operation to support Ukraine through the EU's Cyber Rapid Response Team, which was activated Tuesday. The threat of cyberattacks on European soil is two-fold: First, attacks launched on Ukrainian networks could spread to European networks. Second, Russia could choose to launch direct attacks on European targets through its intelligence services or cybercriminal groups to disrupt the West's response to the Ukraine crisis. Cyberattacks on Ukraine have affected Europe in the past. In 2017, hackers spread malware known as NotPetya through a Ukrainian piece of software and triggered a worldwide cyber crisis seen as the most devastating cyberattack in history. Western security services later attributed the attack to Russia's military intelligence agency GRU. "There is always the threat of a spillover" like NotPetya, said Jaak Tarien, director at the Cooperative Cyber Defence Centre of Excellence (CCDCOE), a NATO-accredited cyber defense center based in Tallinn that advises the defense alliance and its members on cybersecurity. "It's the one internet we're using," Tarien said, pointing to the connections Europe's tech networks have with Ukraine. Baltic countries, in particular, in past years were often the target of campaigns by Russian state-backed hacking groups targeting public and private institutions. The EU attributed a campaign known as "Ghostwriter" at least in part to Russia, after it first plagued Baltic countries with phishing emails and disinformation campaigns and then moved on to target Polish and German politicians. Countries like Estonia and Lithuania have also emerged as vocal proponents of a tougher response to Russian cyber aggression in Europe. Officials in the Baltics are now on high alert, expecting more attacks to come from Russia as the conflict in Ukraine escalates. Last week, Lithuania's Ministry of Defense raised the alarm, saying it expected serious cyberattacks on the country's public authorities. "We definitely see how, as the general state of security deteriorates, the likelihood of cyber activities increases. We're working on a higher alert level," said Margiris Abukevičius, vice minister at the Ministry of National Defense in Lithuania.

## Hybrid War Disinformation

#### Specifically, Russia will use disinformation in order to destabilize the region

Horchakova 2022, Veronika Horchakova Mykolas Romeris University, European and International Business Law program, Master’s degree student(“STRENGTHENING THE TRANSATLANTIC PARTNERSHIP: CHALLENGES AND OPPORTUNITIES FOR THE BALTIC STATES” https://repository.mruni.eu/bitstream/handle/007/18311/Teisines\_minties\_svente-97-107.pdf?sequence=1)

The other non-military threat for the Baltic region is Moscow’s use of the Russophone minority as political instruments against the West. For example, signs of warfare were identified when Russian-speaking inhabitants in Vilnius received brochures with disinformation on the economic situation in Lithuania and a call to participate in the resettlement of ethnic Russians from Lithuania to Russia.13 This kind of propaganda was also used in Ukraine to disrupt loyalty to the State. The Baltic countries need to create a “defensive shield” to fight against Russia’s disinformation and propaganda. Moscow’s primary goal is to form a positive opinion of Russia among local inhabitants by creating dissatisfaction with the relevant governments, shaping and misrepresenting historical facts, and exploiting the vulnerabilities of the Baltic’s political systems, economy, and society. Here the Lithuanian case can serve as a guide for the other two Baltic States and NATO members, too. The roots of the anti-Russian propaganda and disinformation campaign originated in 2016, when Lithuania introduced temporary bans on Russian media outlets that breached pre-existing media laws.14 Shortly after that, the Lithuanian parliament adopted an ordinance restricting Russian media production content on Lithuanian TV. In 2018, the Lithuanian parliament adopted new amendments to the Public Information Law. TV channels in Lithuania must translate TV programs into Lithuanian “if these programs are produced in Russian or other non-EU languages and broadcast for longer than one hour and a half.”15 Such restrictions are effective at diminishing the Russian influence, but are not a panacea. As for cyber security, the Baltic States have undertaken successful work in combating cyber-attacks. According to the International Telecommunication Union’s Global Cybersecurity Index 2020, among 194 countries, Estonia is ranked third after the US and the UK. Followed by the Russian Federation, Lithuania is the sixth-best cyber protected country. Latvia completes the list of the top 15.16 This ranking is based on five pillars: legal, technical, organizational, capacity building, and cooperation measurements related to cybersecurity. Since 2019, these countries have each had Cyber Security Strategies, but we have to consider that these rankings are not always reliable, and sometimes they do not represent reality in all its shapes. Despite establishing the NATO cooperative Cyber Defence Centre of Excellence in 2008 (hosted by Estonia), several commentators have criticized the real cyber warfare capabilities of NATO. In a 2019 interview, the former supreme allied commander of NATO, Adm. James Stavridis, USN (Ret.), warned that “in cyber, and cybersecurity, we have the greatest mismatch between the level of threat and level of preparation.”17 New asymmetric or technological threats require extensive cooperation not only within but also outside of the Alliance. The security and defence sectors in the Baltic States need to build partnerships with the private and academic sectors, all of which will need to cooperate with each other to maintain situational and technological awareness.18 It is clear that, in reality, the ongoing conflict between western countries and Russia does not take place inside tanks or submarines but behind a computer. Russia has massively increased its cyber warfare capabilities and is particularly strong in social manipulation and other cyber-attacks. In this context, there are signs of significant commitment over time to enable the Baltic countries to develop their national defence further. For example, the Baltic States have already signed a five-year roadmap of defence cooperation with the Pentagon,19 meaning that, by 2024, capability development and defence-related aid, training exercises, and cyber defence will be exercised with the US. Officials emphasized the benefits of this program and said that they look forward to its further development. Activated transatlantic relationships are the perfect opportunity for Lithuania, Latvia, and Estonia to generate new partnership programs, agreements, and projects against Russian soft power.

#### Aims to destabilize Baltics separate from NATO makes deterring Russia impossible – now is key after Ukraine

Kols 2022, Rihards Kols Chairman of the Foreign Affairs Committee The Saeima (Parliament) of the Republic of Latvia (3/17/2022 “Hybrid Threats: The Baltic Perspective” https://www.csce.gov/sites/helsinkicommission.house.gov/files/RKols\_Hybrid%20threats%20Baltic%20Perspective-2022.pdf

Since regaining our independence from the Soviet Union in 1990, Latvia, Lithuania, and Estonia have been under constant Russian pressure. This pressure has manifested itself is through the conventional military threat, punctuated by ongoing airspace violations by Russian military aircraft and navy, unannounced, large-scale military exercises of inherently offensive nature along their borders, and the general disposition of Russia's military forces in regions closest to the Baltic borders, doing so under the pretence of counteracting the "hostile West" and promoting militarism. Influence, psychological, and information operations have been part of Russian doctrine since the early days of the Soviet Union, but historically they have been relegated to supporting roles. Nevertheless, as General Gerasimov has observed and thus included in the Russian military doctrine, non-kinetic are exceedingly practical, and these instruments will become dominant in future warfare. This is reflected in most current Russian foreign, security and defence policies and doctrinal documents. For years, the strategic goal of Russian information operations in the Baltic states has been to create distance between the Baltics and the West. The Russian concept is rooted in the idea that democratic societies are vulnerable to political manipulation, and exploiting this perceived weakness is far less costly than pursuing annexation or occupation. Consequently, Russian information operations in the Baltics focus on nine objectives: (1) Encourage and support armed actions by separatist groups to promote chaos and territorial disintegration; (2) Increase polarisation between elites and society to foment a crisis of values followed by process of orientation toward Russian values; (3) Demoralise the military and otherwise attrit resolve; (4) Undermine socioeconomic stability; (5) Engender socio-political crisis; (6) Intensify simultaneous forms and models of psychological warfare to demoralise the Baltic states' armed forces and population and break their resolve; (7) Incite mass panic and degrade confidence in crucial government institutions; (8) Defame political leaders not aligned with Russian interests; (9) and Undermine international alliances and partnerships.12 Russia seeks to achieve its strategic ends in the Baltics through influence operations rather than conventional means. Recognising resistance to deeper ties with Russia in the Baltics, Russia has diversified its messaging beyond pro-Russia content. Instead, the Russian strategy is to attempt to convince members of the population that their countries' current alignment with the West, embrace of democracy, and membership in NATO and the EU are in some way detrimental, degrading or dangerous. Russia heavily leverages Russian and local-language traditional media, social media, and the internet toward this end. There is no universally agreed definition of hybrid threats, considering that a wide range of activities falls under this term. Moreover, hybrid threats evolve constantly, and new means in hybrid warfare emerge. However, the European Centre of Excellence for Countering Hybrid Threats defines hybrid threats as "an action conducted by state or non-state actors, whose goal is to undermine or harm a target by influencing its decision-making at the local, regional, state or institutional level. Such actions are coordinated and synchronised and deliberately target democratic states and institutions' vulnerabilities". 3 The use of hybrid tactics often is based on trying to undermine fundamental democratic values and liberties, and it is done under what some call a "chaos strategy". Russia sows chaos to achieve its agenda beyond its borders by deploying an array of hybrid warfare tools - hybrid warfare is a tactical application of the chaos strategy. Total spectrum warfare deploys a blend of conventional and nonconventional means to affect on the ground changes in target populations or territories while seeking to avoid direct military confrontation. Hybrid warfare is employed in a tailored way to sow chaos in target countries. Such efforts generally include irregular warfare, active measures, and special operations. Like the world, hybrid war is not static, and new tools are developed and employed constantly. For the Baltics, having lived in this environment for the majority of their lives, both under Soviet occupation and after regaining their countries' independence, this multi-vector warfare - hybrid warfare tactics and the chaos they attempt to create, have become intuitively recognisable and often seep into the background like white noise.4 From the perspective of the Baltic states, the development of hybrid threat-related policies at the EU or NATO level has been a natural consequence of the changing security landscape in Europe, especially the gradually deteriorating relations between the West and Russia. In the immediate aftermath of Russia's first attack on Ukraine's sovereignty and territorial integrity, different hybrid attack scenarios against one of the three Baltic states were envisaged, e.g., Russia's attempt to overtake Narva, a city in the extreme eastern point of Estonia, where more than 80% of the population are ethnic Russians; or the so-called "little green men", armed soldiers without insignia that were seen in Crimea in March 2014, entering Latgale, the region in Latvia's east5 ; or Russia creating an incident linked to Kaliningrad – the Russian enclave on the Baltic sea wedged between Lithuania and Poland. In the event of any war between Russia and NATO countries, it is through this gap that NATO would have to rush reinforcements and supplies from Poland to the Baltic countries, and it is this gap that Russia would have to close to prevent that. Military strategists have long suggested that Russian forces from Belarus could attempt to punch across the narrow Lithuanian territory known as the Suwalki Gap to the Moscow-controlled enclave of Kaliningrad, effectively cutting off the three Baltic states. 6 These scenarios included Russia sending troops to "restore order" in case of an uprising in Kaliningrad or sabotaging the train lines across Lithuania that serve as a vital transit corridor from Russia. Because Baltic rail infrastructure is still primarily dominated by Soviet-era rails of a specific gauge width, one incompatible with the EU standard rail gauge width, the risks are substantial enough to cause concern. It has been considered that Russia could use the same pretext as in Ukraine, i.e., protection of the Russian-speaking minorities, to target one of the countries in the region, or rely on state-controlled Russian TV channels widely watched by ethnic Russians in the Baltics to spread propaganda and air true and imagined grievances.7

#### Triggers invasion of the Baltics---escalates quickly

Brent Eastwood 22, Now serving as 1945s New Defense and National Security Editor, Brent M. Eastwood, PhD, is the author of Humans, Machines, and Data: Future Trends in Warfare. He is an Emerging Threats expert and former U.S. Army Infantry officer, January 2022, "Forget Ukraine: Could Russia Invade And Conquer The Baltic States?" https://www.19fortyfive.com/2022/01/forget-ukraine-could-russia-invade-and-conquer-the-baltic-states/ //AShah

We’re Focused on Ukraine But Look Out For the Russian Threat to the Baltics: It was a shot heard around the world in the Russian military analysis community. A RAND Corporation simulated wargame in 2016 concluded that the Russian military could reach the suburbs of the Estonian and Latvian capitals of Tallinn and Riga in less than 60 hours. In the iterations of the exercise, the Estonians and Latvians would need at least seven brigades of troops that include at least three armored brigades to potentially fight the Russians to a standstill.

But it gets worse from here. In another RAND wargame in 2019, the players examined if NATO and Russia would use tactical nuclear weapons during a simulated war in the Baltic states (Estonia, Latvia, and Lithuania). The scenario also had Russian conventional forces over-running capitals in the Balkans and NATO having the last fail-safe option to use non-strategic nuclear weapons.

What Type of Warfare Could the Russians Use Against the Baltics?

A widespread fear is that the Kremlin could use hybrid warfare (conventional and unconventional aspects of power projection) again to annex parts of the Baltics, which would trigger Article V with NATO allies and would require a military response against the Russians from NATO members. A glance at a map will tell you that St. Petersburg is dangerously close to Tallinn, Estonia and Riga, Latvia. But according to General Valery Gerasimov, the Chief of the General Staff of the Armed Forces of Russia, the distinctions between offensive aspects of war and defensive aspects of war are blurring.

Under this Gerasimov Doctrine, the Kremlin then could engineer a Russian hybrid incursion of cyber and information warfare attacks against the Baltics, and these tactics could be made to be seen as a defensive operation. Since the Baltics have ethnic Russians as part of the population, Moscow could employ special operations forces as peacekeepers to protect compatriots. This could happen with an information warfare campaign that would increase the chances for protest and other domestic unrest with ethnic Russians as victims in the Baltics. Then a hybrid operation would ensue to protect ethnic Russians.

According to the two RAND sets of wargames, the Russians would then bring in the heavy armored and mechanized infantry units to “teach the Baltics a lesson.”

#### Disinfo wrecks Baltic stability. Prefer the first and only statistical study.

SEM = structural equation modeling method

Morkūnas 7-12 [Mangirdas Morkūnas, Faculty of Economics and Business Administration, Vilnius University; 7-12-2022; "Russian Disinformation in the Baltics: Does it Really Work?"; Taylor & Francis; https://www.tandfonline.com/doi/abs/10.1080/10999922.2022.2092976; KL]

Introduction

In recent years, awareness of Russian disinformation activities and disinformation efforts has been growing both in the West and in Central and Eastern Europe (Baumann, 2020; Kuczyńska-Zonik & Tatarenko, 2019). Russian disinformation is considered to have achieved some success even in the most developed western countries, where it is presumed to have interfered in the election campaign in the USA (Golovchenko et al., 2020), harassed and impeded independent investigations in Western Europe (Aro, 2016), sought to impair public support for Western assistance to former Soviet countries (Richey, 2018), and significantly affected the election campaign in France (Makhashvili, 2017). Among the main targets for Russian disinformation are the former Soviet Union countries that in Russia are referred to by a unique term coined in 1992, called “near abroad,” (ближнее зарубежье) which attempts to emphasize their status as foreign countries not fully recognized by Russia (Rotaru, 2018). Russian disinformation in the “near abroad” countries seek two main objectives: to inflict as much damage to the statehood of the target countries and to portray Russia in much better colors in the eyes of their citizens (Shakrai, 2015), typically by distorting historical events (Ehrlich, 2021). Although the aim of preventing former Soviet Union Republics from fully diverging from the Russian sphere of influence (Cooley, 2017; Dunn & Bobick, 2014), the Russian Federation has made the Baltic States a target of continuous negative disinformation and psychological subversion tactics (Veebel, 2015), making the disinformation dominated by negative messaging (Thornton & Karagiannis, 2016). It is even stated that among all the European nations, citizens of the Baltic States experience the most concentrated and sophisticated disinformation efforts as an expression of soft power (Simons, 2015). Such Russian disinformation has been affecting the citizens of the Baltic States for more than the past three decades. Arguably residents of the Baltic States are believed to be more susceptible and receptive to various forms of Russian disinformation, having been subject to some 50 years of Soviet brainwashing (Schuhrke, 2019; Thompson, 2019). Such disinformation increases dissatisfaction with domestic governments (Golovchenko, 2022) and the state of democracy generally (Oates, 2016), lowers incentives for personal self-development (Benkler et al., 2018), and provokes anger and social inequality within society (Bardach-Yalov, 2012). There are additional thoroughly documented cases about the intimidation of Baltic States from the Russian side. Matthews (2020) points out at Russian actions aimed at increasing ethnic tensions within these countries. It becomes possible because Baltic States have a significant Russian minority (Best, 2013). Russia is also fully engaged in spreading false information about the possible revision of various treaties between the Baltic States and Russia (Matthews, 2020) up to revoking the recognition of Lithuanian independence (Labanauskas, 2022). Baltic States also have been a subject of various cyber-attacks from Russian based hackers and are expected to experience even more sophisticated cyber-warfare activities it in a foreseeable future (Mälksoo, 2018). The position of Baltic States as a frontline in a cyber-warfare was acknowledged also by NATO by a decision to establish its cooperative cyber-defense competence centre of excellence in one of the Baltic States – Estonia (Kovács, 2018).

In this study the follow the definition of disinformation presented by Bayer et al. (2019). It covers the spreading of information which is designed to be false or manipulated or misleading. It also has the intention of generating insecurity, tearing cohesion or inciting hostility, or directly to disrupt democratic processes (Bayer et al., 2019, p. 18).

Although in recent years, Russian disinformation reached the level of “strategic information operations” (Flanagan et al., 2019), there have been very few studies on the actual effect of such disinformation. Completed studies were based on qualitative evaluations (Surowiec, 2017), focused on Western countries (Carter & Carter, 2021), or investigated only specific issues – mostly the Russia-Ukraine dispute (Gerber & Zavisca, 2016).

Therefore, the present paper aims to evaluate the effect of Russian disinformation on the Baltic States. In order to assess the latent variables related to the effect of disinformation activities on citizens’ minds, this paper uses the structural equation modeling method (SEM), in which a partial least squares technique is employed. To our knowledge, this is the first study on the effect of disinformation on the target countries’ populations using sophisticated statistical methods.

The study consists of several parts: the introductory section provides a brief overview of the aims and impact of Russian disinformation in the Baltics, the “Materials and Methods” section introduces the research model and the hypotheses for the study, and the main results are presented in the “Results” section. Finally, the “Conclusions and Discussion” section summarizes the insights of the study, juxtaposes it with the prevailing theoretical streams, and offers directions for future studies in the subject area.

Theoretical background

There is increasing debate about the socio-political consequences of negative disinformation. Arguably, disinformation enables the success of populist parties during election campaigns (Chernobrov & Briant, 2020) and affects political decisions, as politicians are reluctant to take actions that are potentially unpopular with certain voting groups (Acemoglu et al., 2013) that could be subject to various disinformation tactics (Van Herpen, 2015). Prolonged negative disinformation campaigns lower public participation (Bonch-Osmolovskaya, 2015) through both increased perception of negligibility of voters actions (Van Herpen, 2015) and increased apathy (Gulenko, 2021).

In recent years, the intensity of Russian disinformation has substantially increased, especially on social media (Prier, 2020). One of the main aims of destructive Russian disinformation, which has intensified since 2014, is to discredit national authorities by questioning the independence of their actions or decisions (Lelich, 2014). This leitmotif of the “other hand ruling the government” has also been applied through information warfare against another post-soviet country – Ukraine – and is considered to be highly effective (Karlsen, 2016). It also increases citizens’ perception of hostility with respect to the surrounding environment and diminishes their participation in public life and socio-economic activity (Irisova, 2015). Furthermore, Russian disinformation in post-Soviet states boosts nihilism to substantially undermine the economic activity of their populations, especially with respect to future gains (Julukhidze, 2020). Nihilism as a result of increased distrust provoked by Russian disinformation is mentioned by Paul and Matthews (2019), and Russian disinformation objectives to create and facilitate distrust in Government were also noticed by Sanovich (2017). Disinformation also violates the self-identity and perception of justice (Blouin & Mukand, 2019). Reflections on the exaggerated perception of corruption within the state apparatus were found to be one of the most discussed topics (Miller, 2019). The emphasized narrative of the “failed state” in which everything is decided in advance, and in which citizens can neither influence policy decisions nor be the masters of their own personal or career development, is also important for Russian disinformation architects (Helmus et al., 2018). The disinformation-related influence of diminished motivation for positive, personal development has also been mentioned by Smith and Lasswell (2015).

Attempting to undermine the perception of safety within the country through constant intimidation and threat of imminent military actions is another major tactical aspect of Russian disinformation (Giles et al., 2015). Although in the short term, the effect may be opposite to that expected by the disinformation designers – a consolidation of the nation in the face of immediate aggression (Yurkova, 2018), in the long term, it rewards the disinformation creators in the form of decreased trust in public institutions (Haas, 2017) and the state itself (Redley, 2007) in the target country. Such dual effects of disinformation not only increase the complexity of how it may be detected, (Kausar et al., 2020) but also make understanding its effects even more puzzling.

It has been noted that although Russian state disinformation is very effective within Russia itself by forcing the Russian population to accept a distorted reality, it becomes a counterproductive element outside Russian borders (Belousov, 2012) where it no longer achieves its main objectives (Benkler et al., 2018). These contradictions not only substantiate polemics about the ambiguity of Russian disinformation outcomes but also add weight to arguments in favor of the present study.

In summary, Russian disinformation in the Baltic States is directed at increasing the populations” distrust in their governments (Lough et al., 2014), promoting the perception of a lack of justice (Paul & Matthews, 2016) or career possibilities (Kuczyńska-Zonik, 2017) within the country, and reinforcing the threat of the imminent military action in the region (Buinauskas et al., 2016).

#### Russian disinfo, combined with the threat of invasion destroys the Baltics. It’s the first and only statistical study.

SEM = structural equation modeling method

Morkūnas 7-12 [Mangirdas Morkūnas, Faculty of Economics and Business Administration, Vilnius University; 7-12-2022; "Russian Disinformation in the Baltics: Does it Really Work?"; Taylor & Francis; https://www.tandfonline.com/doi/abs/10.1080/10999922.2022.2092976; KL]

Conclusions and discussion

The present study offers a solution to one of the main issues in disinformation research – the problem of assessing the effectiveness of disinformation (Aggarwal & Sadana, 2019; Oliinyk & Lyasota, 2018). SEM is confirmed to have derived robust results indicating the presence of disinformation influences among the population of target countries.

This study represents the first attempt to clearly document the negative economic outcomes of Russian disinformation within the Baltic States. Such adverse effects were assumed (Molder & Sazonov, 2020), though not yet proven. We discovered that a constant narrative from various information sources related to the imminent nature of military action in or around the Baltic region (Makarychev, 2020; Veebel & Ploom, 2019) harms the economic development of these countries through the reluctance of their citizens to invest in their domestic economies. The erosion of trust in the Government also may have far-reaching implications, including an indirect effect on the economy. The Baltic States are also lagging behind other EU Member States in terms of vaccination against COVID-19. This has also been attributed by some experts to skepticism toward government actions (Genys & Krikstolaitis, 2021). Lower vaccination rates lead to longer and stricter economic lockdowns, higher spending on treatment of infected persons, etc. Weakened trust in the Government in Lithuania, compared to Western States, leads to greater reluctance of the part of the population to seek public institutions’ assistance when facing a crisis; consequently, Lithuania has the highest rate of suicide among European countries (Zalsman et al., 2017).

This study additionally confirmed the strong relationship between the perception of justice within the country and trust in the Government. Although it is considered a prerequisite for a strong democracy (Kashwan, 2017), many countries still have failed to ensure social justice (Lee, 2021). The relationship between perceived career possibilities and trust in the Government indicates a high level of paternalism in Baltic States’ societies, where the governments are expected to display a significant level of care, possibly taking responsibilities that are typically met at the individual level, e.g., career development (Vande Griek et al., 2020).

The perceived threat of war, which is one of the main leitmotifs of the Russian disinformation campaign targeting in the Baltic States (Saxi et al., 2020), is both found to affect trust in the government, thus disrupting social stability and coherence (Klumbyte, 2019), and produce a direct negative economic impact by undermining domestic investment. Contrary to the popular opinion that consistent awareness of possible military intervention helps unify society and win its support for strengthening the armed forces in some of the Baltic States (Romanova et al., 2020), the results of this study add weight to the differing opinion that a significant fear of military threat may have more negative than positive outcomes.

The results of the current study indicate that governments of the Baltic States ought to pay more attention to measures aimed at countering the effect of the disinformation efforts of unfriendly nations, as it affects not only the social landscape but also the economic development of Baltic nations. Governments may be persuaded to counteract Russian disinformation more aggressively than up until the present when counter-disinformation actions were more balanced in favor of ethics (Bjola, 2018). The present study serves as a starting point for more comprehensive studies of the economic and social impact of negative disinformation tactics. In the future, it may be beneficial, both from scientific and applied perspectives, to investigate the impact of disinformation on a wider range of aspects of the economic development of the country in order to develop a more multifaceted and comprehensive understanding of the destructive outcomes of long-term negative disinformation. The deeper research into the methods which are being used by Russia for disinformation campaigns could also help to better understand and counter the effects of disinformation campaigns and to minimize its negative impact.

### Cyber---Hybrid

#### NATO cybersecurity cooperation solves Russian propaganda and Baltic resilience.

Kühn 18 [Ulrich Kühn, nonresident scholar at the Carnegie Endowment for International Peace, and a senior research associate at the Vienna Center for Disarmament and Non-Proliferation (VCDNP)/James Martin Center for Nonproliferation Studies, based in Vienna, Austria. Previously, he was a Stanton Nuclear Security Fellow with Carnegie’s Nuclear Policy Program, and a fellow with the Institute for Peace Research and Security Policy at the University of Hamburg (IFSH). He holds a PhD (summa cum laude) in political sciences from Hamburg University, an MA in Peace Research and Security Policy from Hamburg University, and a Magister Artium in medieval and newer history as well as German literature from the Rheinische Friedrich Wilhelms University Bonn. His current research focuses on NATO-Russian relations, transatlantic security, nuclear and conventional deterrence and arms control, and the proceedings of the OSCE. Kühn worked for the German Federal Foreign Office and was awarded United Nations Fellow on Disarmament in 2011. He is the founder and a permanent member of the trilateral Deep Cuts Commission and an alumnus of the ZEIT Foundation Ebelin und Gerd Bucerius; 3-28-2018; “NATO’s Options”; *Preventing Escalation in the Baltics: A NATO Playbook*, Carnegie Endowment for International Peace; https://carnegieendowment.org/files/Kuhn\_Baltics\_INT\_final\_WEB.pdf; KL]

RESILIENCE

Unlike the threats Russia poses in the military realm, Moscow’s intimidating NATO allies through nonkinetic operations across various civilian domains cannot be countered by traditional military means. Instead of deterrence and defense, civilian resilience measures are better tools for dealing with most of Russia’s NGW tactics. In particular, increasing the resilience of ethnic Russians in the Baltic states to Russian propaganda should become a key feature of NATO policy. The example of Ukraine, though very different compared to the three Baltic states, shows that existing ethnopolitical tensions can serve as a gateway for Russian intervention.

In Ukraine, Russia exploited existing ethnopolitical problems as a pretext to resort to the use of force. Its methods should lead to two important realizations: the Kremlin cares about its image on the global scene, and it is mindful that any narrative justifying intervention should receive broad domestic support in Russia.9 Both realizations have implications for managing deliberate as well as inadvertent escalation pathways. Prior to an act of aggression against NATO, Moscow would have to create a pretext of a magnitude that would justify war with the world’s most powerful military alliance. While that seems unlikely, one cannot exclude the possibility that unrest in the Baltics involving minority ethnic groups could lead to inadvertent escalation if domestic pressure mounts in Moscow. For NATO, there are not many military options for mitigating these escalation risks. Deterrence is only applicable in so far as Russia decides to react to a domestic crisis in the Baltics—deliberately instigated or randomly occurring—with military pressure or the use of force.

A more effective approach would be to reduce the initial risk of domestic unrest as much as possible. Resilience measures could be an important way to help make minorities more immune to nonkinetic Russian operations, such as propaganda and disinformation. However, NATO’s current efforts to strengthen resilience focus on preventing disruption to military deployments to ensure effective deterrence and defense.10 Beyond the military realm, NATO treats resilience as one facet of its efforts, not a core task.

But NATO has several options as its disposal to broaden its resilience portfolio. To begin with, NATO could provide technical assistance funds to the Baltic states to help them build Russian-language media outlets from the ground up. This assistance should cover capacity building, program development, public relations, and branding. To be comprehensive, these efforts should include traditional media outlets—such as newspapers, television, and radio—as well as social media and internet resources. The aim would be to provide a counternarrative to Russian propaganda and help audiences distinguish between facts and fake news.

While such efforts to build resilience would be much cheaper than most military options, any positive effects would only be seen in the coming decades. At the same time, allies might struggle to reach a consensus on whether NATO, a military alliance, is really the right organization for a soft power approach, not least because such efforts would run the risk of being seen as NATO-sponsored propaganda. Since NATO already cooperates with the EU on resilience,11 Brussels would, perhaps, be better placed to lead such efforts.

The contentious debate about NATO members’ goal to spend 2 percent of their GDP on defense may unleash positive synergies. Certain allies, including Germany, argue that nonmilitary measures such as post-conflict reconstruction, conflict prevention, development aid, and the integration of refugees contribute to allied security and that NATO should count spending on them toward the 2 percent target.12 Even though NATO’s secretary general has rebuked German calls,13 allies could make a virtue out of necessity by encouraging Germany and others to finance and organize independent Russian-language media outlets and recognizing that such resilience efforts count toward the target.14

Another option for NATO could be to closely monitor the state of integration, rights, and treatment of Russian minorities in the Baltics, and to intervene, perhaps through a special civilian monitoring and advisory mission, in cases of concern. Such a watchdog institution could help signal to Russia that NATO is taking the issue seriously. NATO does not currently play a role on minority rights within member states and is wary about infringing on members’ sovereignty. It could, therefore, be quite difficult to reach a consensus about allowing NATO to intervene directly in the domestic policies of its member states. Allies with a poor track record in terms of democratic institutions and the rule of law, including Turkey or Hungary (and, to a lesser extent, Poland), might even view this as a dangerous legal precedent. In addition, institutionalized monitoring might inadvertently come across as exactly the kind of stigmatization of the Baltic countries that Russia wishes to generate.

But NATO is an alliance of shared values, and the integration and fair treatment of Russian minorities in the Baltic states is too important a matter to leave unattended. If allies found NATO monitoring to be unacceptable, they could opt for self-reporting. Obviously, self-reporting by the Baltic states would have its weaknesses, but such an approach could be accompanied by behind-the-scenes pressure from other allies to ensure reports were meaningful. Another option would be to task the OSCE, which is also concerned with human rights, with an enhanced monitoring role. The problem there, however, is that Russia has a veto in that organization.

Increasing the resilience of NATO members against Russian meddling should not stop with the Baltic states. As Russian attempts to interfere in the elections of France, the Netherlands, and the United States have all shown, strengthening the cyber defenses of governmental agencies as well as political parties is a first necessary step to prevent the deliberate leaking of confidential information. NATO should make national resilience measures in the cyber realm count toward the alliance’s 2 percent defense spending target.

Furthermore, allies need to make their publics aware that they are being influenced by Moscow, either directly or through proxies. Since a growing number of citizens treat their own governmental institutions with skepticism, national governments should cooperate, by sharing information about Russian interference, with independent civil society groups that are often seen as more credible. This approach carries the risk of looking like collusion, but it is a risk worth taking. One of the downsides of NATO focusing so heavily on Russia over the last few years, though entirely warranted, is a tendency to portray the Kremlin as an undefeatable “superman,” which it clearly is not. Allies could therefore send a more determined public message to their own populations that what Moscow is doing is neither new nor significant enough to bring down Western democracy and the rule of law.

#### Hybrid attacks escalate. Miscalc and Putin’s motivations make it likely.

Tol et al. 22 [Jan van Tol, Senior Fellow at the Center for Strategic and Budgetary Assessments. Prior to his retirement from the Navy in 2007, Captain van Tol served as special advisor in the Office of the Vice President. He was a military assistant to Andrew W. Marshall, the Secretary of Defense’s Principal Advisor for Net Assessment, from 1993–1996 and 2001–2003. At sea, he commanded three warships, two of which, USS O’Brien (DD-975) and USS Essex (LHD-2), were part of the U.S. Navy’s Forward Deployed Naval Forces based in Japan. Captain van Tol’s analytic work has focused mainly on long-range strategic planning, naval warfare, military innovation, and wargaming. He holds a B.A. in Philosophy and Logic from the University of Massachusetts/Amherst and a M.S. in Operations Research from the Naval Postgraduate School, and graduated with distinction from the College of Naval Command and Staff at the U.S. Naval War College; Christopher Bassler, Senior Fellow at the Center for Strategic and Budgetary Assessments, where he researches technology & innovation, joint aerospace capabilities, maritime operating concepts, and overall U.S. & allied military strategies. He served as a civilian in the Department of Defense, for both the Departments of the Navy and the Air Force, as an engineer, designer, strategist, and advisor. His previous assignments include the F-35 Joint Program Office, the Office of the Chief of Naval Operations (OPNAV) in the Pentagon, the Office of Naval Research, and the Naval Surface Warfare Center, Carderock Division. He has worked in various capacities to enhance capabilities and interoperability across all warfighting domains, in many technology areas, and with key allies and partners on five continents, including NATO for both the capabilities and the S&T Organisation. He was awarded two U.S. Patents. Dr. Bassler received two U.S. Navy Meritorious Civilian Service Awards, from the U.S. Secretary of the Navy and the Chief of Naval Research. His degrees include a Ph.D. in Aerospace Engineering from Virginia Tech; a M.A. in Security Policy Studies from the George Washington University Elliott School of International Affairs; and a Diploma in Strategy & Innovation from the University of Oxford, Saïd Business School; Katherine Kjellström Elgin, Fellow at the Center for Strategic and Budgetary Assessments. She brings rigorous research to policy discussions and has held positions in both academic and policy organizations. Prior to joining CSBA, she served as a DAAD Post-Doctoral Fellow at the Foreign Policy Institute of Johns Hopkins School of Advanced International Studies (SAIS), where she wrote and published on grand strategy, great power relations, U.S. defense strategy, European security, and alliance management. Dr. Elgin has also worked at the Brookings Institution and with the Long Term Strategy Group in Washington, D.C. In 2018, she served as a visiting fellow at the Institute for Security & Development Policy in Stockholm, Sweden. Dr. Elgin earned her Ph.D. in Public Affairs (Security Studies) from Princeton University’s School of Public & International Affairs. At Princeton, she served as the director of the Center for International Security Studies’ Strategic Education Initiative, leading the university’s program for educating and mentoring students with an interest in national and international security; Tyler Hacker, Analyst at the Center for Strategic and Budgetary Assessments. His work focuses on U.S. defense strategy, future warfare, and great power competition. Prior to joining CSBA, Tyler was an analyst at the Congressional Research Service, where he conducted research on topics in defense logistics. Tyler previously served as a field artillery officer in the United States Army in Germany, where he participated in NATO operations and exercises in Poland, Romania, and the Baltic states. He has also completed internships at the U.S. Army War College and the American Enterprise Institute. He holds a B.A. in International Studies from Virginia Military Institute and an M.A. in Security Studies from Georgetown University; 2022; "Executive Summary"; *Deterrence and Defense in the Baltic Region: New Realities*, Center for Strategic and Budgetary Assessments (CSBA); https://csbaonline.org/uploads/documents/CSBA8312\_(Deterrence\_Defense\_Baltic)\_web.pdf; LR + KL]

New Realities

Vladimir Putin’s invasion of Ukraine on February 24, 2022, came as a shock to many observers. Few countries in Europe felt affected by the invasion of Ukraine as much as the Baltic states, which each directly border Russia, Belarus, or both. They, as well as Poland, had been warning about the threat of Russian revanchism from the time of their accession to NATO, but largely to deaf ears within the rest of NATO. Although the Russian seizure of Crimea in 2014 and aggression in the Donbas region of eastern Ukraine prompted calls for change within NATO, the practical response was limited. The invasion and savage ongoing fighting since then have brought to light various new realities that the Baltic region, NATO, and the United States will have to contend with going forward.

The Russian invasion of Ukraine is a forceful demonstration of Putin’s desire and, critically, willingness to change the European security environment through the use of force. It is important to recognize that he has long considered Ukraine to be an inseparable part of Russia itself. Indeed, Putin has long contended with near-messianic fervor that Ukraine is not a sovereign nation.1

Beyond Europe, the Kremlin is dissatisfied with the global order more broadly.2 Indeed, Russia under Putin seeks to shape both the European regional order and the global international order to reestablish its great power status, reclaim its sphere of interest, and expand its strategic depth against NATO.3 It sees the current European security architecture as illegitimate, having been established during a period of Russian weakness. Now, as Putin perceives Russia’s power to have been re-established, he seeks to reassert its strength and re-negotiate the regional order. Russia sees NATO and especially the United States as threats to its national security. One of Putin’s key goals has been to fracture NATO’s political and military cohesion and manifest a clear example of NATO’s dysfunction and waning relevance. Thus, in an effort to both limit the threat that NATO is perceived to pose and to improve its own relative strategic position, Russia seeks to weaken the Alliance and the West more broadly.

Demonstrated Willingness to Use Military Force

The ongoing war in Ukraine demonstrates unequivocally that Russia under Putin is willing to undertake highly risky and costly measures to achieve his strategic aims. Although the war has thus far taken place outside of NATO borders, Putin has demonstrated the willingness to use military force on a large scale to invade another state to achieve his aims. The NATO alliance and its member states accordingly must adapt to the enhanced possibility that in the future Russia may choose to employ military force to attack one or more NATO member states if and when it determines such action to be advantageous.

In recent years, the Kremlin has continued its efforts to weaken the Baltic states through various sub-conventional methods of conflict, including political warfare, information operations accusing Baltic governments of discriminating against ethnic Russians, unfavorable energy pricing, regular violation of Baltic state territorial waters and air space, and the abduction of an Estonian security officer in 2014. Although Russia has not directly threatened the Baltic states with military action to date, the risk of military conflict cannot be written off since the risks of deliberate Russian provocations or of miscalculation are high.4

Besides miscalculation, other circumstances could motivate Putin to threaten or actually undertake military actions against one or more Baltic states. Such actions could take the form, for example, of cross-border incursions, temporary or prolonged seizure of small bits of Baltic state territory, attacks against selected Baltic state military and/or critical infrastructure targets or, in the worst case, full-scale invasion and occupation.

Such circumstances could arise from Russian threat perceptions or, alternatively, perceived opportunities to improve Russia’s self-assessed strategic position. For example, Putin could seek to take advantage of Baltic domestic insecurity—e.g., rising tensions between ethnic Russian minorities and the governments in Estonia, Latvia, or (to a lesser extent) Lithuania—to foment or escalate domestic tensions in order to intimidate the governments or gain influence within those countries.5 Alternatively, Russian perceptions that NATO was attempting to harass or isolate Kaliningrad could lead Russia to employ military force to assure its land line of communications with that exclave. Russian perceptions of a growing NATO military threat in the Baltic Sea or the Gulf of Finland could lead Russia to respond with military activities with the consequent risk of miscalculation between opposing forces operating in close proximity. Russia could also conduct limited incursions to test NATO’s resolve and potentially undermine the credibility of collective defense.

#### Accident risks are high.

Martin and Maynes 22 [Rachel Martin and Charles Maynes, NPR reporters; 6-30-2022; "Tensions are on the rise between Russian and Europe's Baltic region"; NPR.org; https://www.npr.org/2022/06/30/1108843823/tensions-are-on-the-rise-between-russian-and-europes-baltic-region; KL]

The Kremlin is threatening to retaliate against NATO member state Lithuania, after the Baltic state decided to block some goods into a Russian territory known as Kaliningrad.

RACHEL MARTIN, HOST:

As the war in Ukraine stretches into month five, things are getting more precarious for other former Soviet republics. Lithuania decided to block some goods from getting into a Russian territory known as Kaliningrad. And now the Kremlin is threatening to retaliate. Lithuania, we should note, is a member of NATO, so there is a lot of dangerous potential in all this. NPR's Charles Maynes is currently in Kaliningrad. And he joins me now. Hey, Charles.

CHARLES MAYNES, BYLINE: Hi there. Morning.

MARTIN: So set this up for us by explaining more of this territory, Kaliningrad, and how it has become this source of tension right now.

MAYNES: Sure. You know, Kaliningrad is a territory that was seized from Germany and became part of the Soviet Union - along with the Baltic nations of Lithuania, Latvia and Estonia - at the end of World War II. Only amid the push for independence of those countries and breakup of the USSR in 1991, you know, Kaliningrad became something of an island. You know, today, it's called an exclave. It's a separate bit of Russian territory sandwiched between Lithuania and Poland, which are both, of course, now European Union and NATO members. But these recent tensions with Kaliningrad, they really stem from Russia's military campaign in Ukraine and resulting Western sanctions. The problem here is that Lithuania is also applying those sanctions to goods travelling from mainland Russia through its territory into Kaliningrad. The Kremlin says that's illegal.

MARTIN: OK, so lots of complications in all of this. You're on the ground there. What have you been hearing from people?

MAYNES: Yeah. You know, so far, the ban only impacts select goods, like steel, cement, furniture. And as a result, there is an outsized impact on select industries, like construction and shipping. And that's a point that was made to be - made to me by Yakov Grigoriev, who works in logistics here.

YAKOV GRIGORIEV: (Non-English language spoken).

MAYNES: So here, Grigoriev says the ban means it costs more to transport goods. And it takes longer because the only choice is to send everything from Russia across the Baltic Sea now. You know, meanwhile, others I talked to say, look; we want good relations with our neighbors. But this is an unfriendly act against Kaliningrad in particular. And some long-time residents, like Alexander Sokolov, have theories why.

ALEXANDER SOKOLOV: (Non-English language spoken).

MAYNES: So Sokolov here says that friends in Lithuania tell him their media portray Russia as about to attack their country. And he says that couldn't be further from the truth. But by building conflict with Russia, he argues, the authorities in Lithuania can attract additional money and support from the EU and NATO.

MARTIN: So what is Russia going to do?

MAYNES: Well, you know, the Kremlin is issuing not so vague threats against Lithuania. Local officials here have a more nuanced take, you know? They say, yes, Lithuania's actions are an inconvenience. But they can work around them by expanding overseas shipping with more boats.

MARTIN: OK. So if we take a step back here, what does this move by Lithuania mean in the bigger picture when we think about Russian aggression into Ukraine and any potential threats into the Baltic states and Europe?

MAYNES: Yeah. On the one hand, it looks like it's an isolated incident, right? Lithuanian officials say, look; most goods, at least for now, can still pass through Kaliningrad, as they always have. They're just enforcing EU sanctions policy. Less clear is whether the EU entirely agrees, you know? Amid these tensions, the EU is now suggesting they create a carve-out for goods going to Kaliningrad. Meanwhile, Lithuania says it's suddenly facing cyberattacks and bomb threats. We've also seen Russia carrying out drills among its Baltic Sea fleet. And until this issue of transit goods to Kaliningrad is resolved, the problem is just another among many that could trigger an unintended conflict between NATO and Russia.

#### War’s likely now.

Brooke and Stradner 22 [James Brooke, visiting fellow at the Foundation for Defense of Democracies with a focus on Ukraine; Ivana Stradner, adviser at the Foundation for Defense of Democracies; 6-29-2022; "It’s Time for NATO to Help the Baltics "; The Dispatch; https://thedispatch.com/p/its-time-for-nato-to-help-the-baltics; KL]

A new flashpoint between NATO and Russia’s new expansionism flared up after Lithuania banned the transit of sanctioned goods from Russia to Kaliningrad, its exclave on the Baltic Sea, as part of the EU’s sanctions regime that took effect on June 17. Russia called Lithuania’s actions “hostile” and threatened “serious” consequences.

Undeterred, Lithuania this weekend blocked an EU motion that would have nullified the restrictions. Vilnius said that the EU must not succumb to Russian pressure and compromise on its sanctions package.

NATO leaders meeting in Madrid this week should back up Lithuania’s move to put Russia on the defensive. As a larger strategy, NATO should follow Lithuania’s lead of pressuring Moscow and calling out Moscow’s empty threats.

The Kremlin has already responded to Lithuania’s restrictions with information warfare and cyber subterfuge. On Monday, a Russian-speaking hacking group known as Killnet claimed responsibility for part of what Lithuania’s Defense Ministry calls an "intense, ongoing" cyberattack against government and private websites.

This cyberattack tracks with Russia’s Ministry of Defense Spokeswoman Maria Zakharova’s warning that Russia’s response would be “not diplomatic, but practical.” Kremlin spokeswoman Dmitry Peskov was similarly critical of the transit restrictions, calling them “illegal.”

But the restrictions are in strict accordance with EU law. Lithuania blocked only the transit of EU-sanctioned goods, like "metals, coal, construction materials, and high-technology products to the Russian sea port." Lithuania’s Foreign Ministry issued a statement Monday saying that “the transit of passengers and non-sanctioned goods to and from the Kaliningrad region through Lithuania continues uninterrupted.”

The Kremlin threats come as Putin is increasingly open about his expansionism. On June 9, in a new justification for Russia’s war on Ukraine, Putin drew an analogy with Peter the Great’s 21-year war with Sweden. He said: “Clearly, it fell to our lot to return and reinforce [ex-Russian lands] as well.” One week later, at the St. Petersburg International Economic Reform, Putin asked the world: “What is the Soviet Union? It is historical Russia.”

Thirty years ago, the Soviet Union disintegrated into Russia and 14 separate countries. Today, in Moscow, Kremlin-friendly media commentators increasingly call these 14 nations, including Ukraine, “quasi-states.” Spoiling for a fight, Putin looks around the map for a quarrel – or a conquest. By keeping Russia on a war footing, Putin justifies his dictatorship, keeping Russia governable with emergency decrees.

#### Hybrid war escalates.

Wierenga 22 [Louis Wierenga, Junior Research Fellow, Johan Skytte Institute of Political Studies, University of Tartu | Lecturer in International Relations, Department of Political and Strategic Studies, Baltic Defence College; 2022; "Cybersecurity and Hybrid Threats in the Digital Baltic States: A state of the art"; *Hybrid Threats in Baltics and Taiwan: Commonalities, Risks and Lessons for Small Democracies*; https://www.baltdefcol.org/files/files/publications/Hybrid%20Threats\_LIIA.pdf#page=58; KL]

In a very recent and insightful study on AI for digital warfare, Hageback and Hedblom (2022) in their synonymous monograph pose a fascinating question: what Clausewitz would have thought of digital warfare.1 Hageback and Hedblom (2022) then correctly note that the new digital technology which we are now in possession of has led way to a new digital sphere which substantially increases the speed, reach, stealth, precision, diffusion, and breadth of a potential attack.2 Much has changed in the realm of cybersecurity and cyberwar since academic literature first took note.

There is broad consensus amongst academics and policy makers that the nature of warfare and security is changing.3 While this is not disputed, and warfare changes and progresses with time, this claim should be placed within the broader notion of a changing geopolitical landscape and a multipolar world order and in light of Hageback and Hedblom’s (2022) aforementioned observation, relating to digital warfare and cyber conflict. Moreover, there is a growing consensus that within renewed great power competition, the likelihood of a ‘great power war’ is enough to resurrect old fears and direct contemporary security debates. Hybrid warfare usually precedes kinetic warfare or take place simultaneously.4 The targets of acts of hybrid aggression tend to be small states which are geographically near greater powers which seek to dominate them.5

Thus, this article focuses on cybersecurity and hybrid threats facing the three Baltic states, collectively known as Estonia, Latvia, and Lithuania. First, I provide a brief overview of the development of cyber security and hybrid threats in the region, and a brief synopsis of the current state of affairs and conclude by offering some policy recommendations. Although the Baltic states are small states, they carry a big stick when it comes to dealing with cyber and hybrid threats. This can be used as an advantage not only internally when dealing with hostile actors in cyberspace, but when bolstering their voice within NATO and the EU. Estonia has been active in doing precisely this and Lithuania and Latvia are also answering the call.

The development of cybersecurity in the Baltic states: Primary challenges, risks, and lessons learned

Estonia, the small Baltic nation of just over 1.3 million people, certainly packs a big punch when it comes to all things digital, becoming the world’s most advanced digital society. The small, digital nation suitably markets itself as ‘e-Estonia’, with a center bearing the name. Collectively, the three Baltic states fare very well in cyber-preparedness. All three are ranked by the Global Cybersecurity Index (GCI) in the top 20 out of 193 countries. Estonia places third, after only the United States and the United Kingdom.6 Lithuania is ranked 6th, whereas Latvia is further down, ranking fifteenth.7 Lithuania and Estonia rank very high in the National Cyber Security Index (NCSI), among the top ten,8 whereas Latvia is slightly behind, placing 25th. 9

The aforementioned rankings are both impressive and encouraging. However, an alarming ranking to be placed within is the ten counties which are most likely to experience brute-force attacks on Remote Desktop Protocol (RDP) services.10 RDP brute-force attacks account for over 80 percent of all network accounts in each of the Baltic states.11 Yet, the Baltic states remain vigilant.

Within the short history of the Baltic states, post-occupation, it has usually been Estonia leading the charge. However, this is not always the case. For instance, in 2019, Latvia was among the first countries in Europe to launch 5G (fifth generation) for commercial use and a year later opened the first military 5G test site in Europe, located at the Ādaži military base.12

Lithuania has also been incredibly proactive in facing up to cyber threats. A recent initiative in the summer of 2021 was the establishment of the Regional Cyber Defence Centre (RCDC).13 The RCDC operates under the Lithuanian Ministry of National Defence. The RCDC relies on bilateral partnerships. Most strongly with the United States, as well as with Ukraine and Georgia.14 The RCDC is one of two cyber defence centres in the Baltics, the other being the NATO Cooperative Cyber Defence Centre of Excellence (CCDCOE) in Tallinn.

It is hard to separate technical innovation from what history has taught the Baltic states, in terms of facing larger powers with nefarious intentions and a faulty understanding of territorial integrity. Many academics and policy makers and think tankers have noted the change in the global power balance, the changing nature of warfare15, as well as the growing importance of cyberspace as a battleground.16

In 2015, Richard Stiennon warns in his book which bears the candid title “There Will be Cyberwar” of precisely this. Stiennon ends his 2015 publication highlighting geographical hotspots of potential conflict: the loss of Taiwan, naval defeat in the South China Sea, and the loss of territory and sovereignty in Eastern Europe to Russia.17

If 2007 was the initial alarm bell for cyber and hybrid threats in the Baltics, 2020 and the onset of the global COVID-19 pandemic marks another notable date. Two important reasons underlie this. First, due to the lockdowns and social distancing practices enacted across most of the globe and in all Western democracies, education, higher education and a great degree of business was moved online.18 Therefore, online platforms became ‘the new normal and were utilized to a much greater extent, leading to the possibility of greater cyber threats. In the EU, major cyberattacks jumped from 146 in 2019 to 304 in 2020.19 This is something that Welscher (2021) argues has both reshaped cyberspaces as a whole and presented new threats to the Baltic states.20 There has been time to catch up and adjust. However, initially, due to the rapid move online, security became an afterthought in much of Europe.21 Cybercrime increased losses on a global scale by more than 50 percent, hitting also the Baltic states.22 This highlights the dire importance of remaining not just cyber-prepared, but one step ahead.

Second, and pertaining to hybrid and information warfare, both the increased amount of time people spend online during the ongoing pandemic as well as the ripe nature of a crisis of such magnitude for the spread of misinformation, disinformation, and conspiracy theories highlight crucial vulnerabilities. A 2021 report for the European Commission found, perhaps unsurprisingly, that the COVID-19 pandemic served as a catalyst for conspiracy theories.23 This at a time of extreme political and social polarization, coupled with preference bubbles and echo chambers, which allow misinformation and disinformation to both travel and be accepted by a wider audience. Though, with threats also come solutions, better resilience, and the possibility for a united front and further cooperation with allies.

In light of power competition vis-à-vis cooperation with the US, NATO, and the EU, and small states standing up to larger powers with nefarious intentions, the drawback is that no entity is capable of defeating all cyberattacks; rather, in order to succeed in cyberspace, the key is learning how to adequately cope.24 When it comes to information warfare, and one of the reasons for which it is so dangerous, is that the antagonist need not win – they succeed if they are able to successfully cloud the issue.25 It is no secret that Russia has waged numerous information warfare campaigns in the Baltics and show no sign of giving up.

#### Critical infrastructure escalates.

Juurvee 22 [Ivo Juurvee, Head of Security & Resilience Programme and Research Fellow at the International Centre For Defence and Security; 2022; "Energy and Critical Infrastructure Security: The Case of the Baltic States"; *Hybrid Threats in Baltics and Taiwan: Commonalities, Risks and Lessons for Small Democracies*; https://www.baltdefcol.org/files/files/publications/Hybrid%20Threats\_LIIA.pdf#page=38; KL]

THREATS AND DANGERS

There are mainly three kinds of threats to critical infrastructure – emanating from nature, technology failures (usually mixed human error), or hostile action. All these have shaped the understanding of the public, as seen from the discussions in the press, and mainly the last one is reflected in strategy documents in the Baltic states.

With the highest peak of only 318 m over sea level, the Baltic states are flat. The countries are not situated in a seismically active region, neither are they threatened by tsunamis or tornados. However, there are still some natural hazards to critical infrastructure and power supply, mostly caused by the cold or stormy Northern European weather. While floods are usually not dangerous and at some places even considered to be a tourist attraction (Pamarys region  in Lithuania and Soomaa in Estonia), the autumn and winter storms can be more dangerous, especially in Estonia. While short term power cuts and the inaccessibility of roads are usual and appear every year with both the authorities and population well prepared for them, from time to time things get more extreme. In December 2010, almost 600 people were stuck in their cars in the snowstorm on Tallinn– Narva road. One of the main roads of the country was blocked for a day and it was a close call that nobody froze to death. Rough weather in Southern Estonia in December 2019 disrupted the power supply of over 50  000 clients and took days to fix. However, although events like these do happen in the Baltic states, they do not have disastrous effects on infrastructure.13

The COVID-19 pandemic has brought different kinds of problems, although also emanating from nature. The closure of some borders, especially at the beginning of the pandemic in spring 2020, showed the international transport connections – and therefore vital supplies – of the Baltic states may be at risk. Secondly, the pandemic revealed that compulsory self-isolation of persons having been in contact with an infected person might lead to unexpected consequences in companies providing vital services, since many jobs needed to keep the critical infrastructure maintained and smoothy functioning cannot be run from a distance.

Technological accidents (except the sinking of m/s Estonia caused by technology failure and extreme weather conditions in 1994, which was a part of international transport connecting Tallinn to Stockholm) have not seriously influenced the critical infrastructure, however, all countries are situated within the range between 500 to 1000 kilometres from the Chernobyl Nuclear Power Plant, the place of the humankind’s worst technological disaster back in 1986. It has held the threat perception high, especially in Lithuania, even more so since Belarus has built the Astravec Nuclear Power Plant just on the other side of the border, only some 40 kilometres away from the capital Vilnius.14

Most threats, both to security in general and critical infrastructure in particular, are perceived to originate from hostile intent. Although the New York attacks of 2001 were noticed and taken into consideration in the Baltics,15 there have been no serious incidents defined as terrorist attacks (although bomb explosions, usually with criminal motives, were rather common in the 1990s). Still, there have been acts of Islamist terrorism in Northern Europe.

Other hybrid threats are more plausible. Russia’s aggression against Georgia in 2008 and Ukraine since 2014 have made these threats perceptible for both the decision-makers and the public. However, the Baltic states have some experience in materialising hybrid threats. In 2007, Estonia was under diplomatic, economic and informational pressure from Russia, which also applied its secret services and proxies, leading to riots in Tallinn in late April. These activities climaxed with the wide spectrum of cyberattacks against targets in Estonia – the first such occurrence becoming more common in the following years.16 Lithuania – and to a lesser extent Latvia –were hit by Belarus deliberately directing migrant flow to their borders, also accompanied by a massive information campaign, in 2021.17 At the time this article is written it cannot be stated that the crisis is over.

There have been some concerns lately over security aspects of the People’s Republic of China (PRC) foreign investments into critical infrastructure. The concerns have involved 5G technology, but also the transport infrastructure. There was an initiative to build a railway tunnel using PRC investments, technology and labour between Tallinn and Helsinki as an extension of the Rail Baltica line, and therefore of importance to all Baltic states. However, it was turned down by the Finnish and Estonian governments in April 2021, after finding the offer suspicious. If the implementation of the tunnel idea continues, it will be handled in cooperation between the abovementioned governments.18

RECOMMENDATIONS

The need for securing the critical infrastructure has been well acknowledged in the Baltic states and has been progressing, however, no system is perfect.

While planning and implementing measures to secure the critical infrastructure, the whole spectrum of natural and technological threats must be kept in mind. Last not least, threats originating from hostile action from state and non-state actors – hybrid threats – are to be considered. Due to their geographical location, natural disasters have a low probability in the Baltic states, on the other hand, the same location causes a rather high probability of hybrid threats.

The most critical infrastructure systems for modern societies are power supply and IT systems, their security is paramount to keep everything else running. Securing their continuity of operation and resilience against foreign influence by politically manipulated restrictions on supply, cyber and physical attacks is crucial.

To secure the resilience of vital services, smooth coordination between different countries, state agencies and private critical service providers is needed. Of course, it must be regulated and planned, but to be sure, it works, and overcoming the bottlenecks not foreseen by regulators and planning the exercises regularly is also of utmost importance. These should involve – not necessarily at the same time – all levels from the decision-makers in the governments to the first responders on the field or, for cyberspace, behind the screen.

### Cyber---China

#### China cyberattacks the Baltics.

LRT 20 [Lithuanian National Radio and Television (LRT), the Lithuanian public broadcaster is the media group that is owned by the public; 5-13-2020; "Latvian intelligence names China, Russia a threat"; https://www.lrt.lt/en/news-in-english/19/1177615/latvian-intelligence-names-china-russia-a-threat; KL]

Latvia’s yearly security assessment named China a growing cyber and espionage threat, alongside risks posed by Russia’s historical revisionism and foreign policy. Warsaw Institute, a think tank in Poland, analyses the report.

Chinese influence in the Baltics

At the end of April, the Constitution Protection Bureau (SAB), Latvia’s most important intelligence service, published an annual report, reviewing threats to the national security of their country.

A major part of the report concerned the threat from the Russian Federation, but there were also several references to the increasing influence and attacks from China.

In comparison, China was not mentioned in the 2017 document at all, and in 2018 Beijing’s cyber operations aimed at obtaining data, mainly through economic intelligence, were mentioned.

China, on a par with Russia, was mentioned as the main cyber threat to NATO and the European Union.

According to the report, the number of Beijing’s cyber attacks is gradually increasing and poses a serious problem for the security and interests of Latvia and other Western countries. SAB analysts estimate that this trend will continue.

Over the last five years China has invested in tools to organise, centralise and streamline cyber activities. Hacker groups controlled by the Chinese secret services have evaluated their operational methods and improved their technical tools. The report also notes that China’s cyberspace operations have become more technically sophisticated and difficult to detect.

China’s cyber attacks also threaten the economic interests of the West. Such operations are carried out against public institutions, private companies, the academic community, government institutions, the military and defence sector and non-governmental organisations.

The most common motive for attacks is to increase the competitiveness of China’s economy. However, there is also a significant increase in attacks on foreign and security policy-making institutions, which are aimed at obtaining information about policies and plans of countries that Beijing sees as strategically important.

### escalates

#### The Russian Baltic cyber threat will escalate---internal documents prove intent and capabilities

Fraszka 20. Bartosz Fraszka is a graduate of the Centre for Europe and the Faculty of Political Science and International Studies at the University of Warsaw. He also studied at the Euro-American faculty of the Institut d’Études Politiques in Reims. “Baltic States Versus Russian Hybrid Threats”; Warsaw Institute; October 26, 2020; <https://warsawinstitute.org/baltic-states-versus-russian-hybrid-threats/> //BY

Russia’s annexation of Crimea in March 2014 corroborated Moscow’s imperialist pursuits to restore its role amongst the world’s actors it had lost after the collapse of the Soviet Union in 1991. The Crimea case seems now a good starting point for current thoughts on the very essence of hybrid threats. This is what pushed the Baltic republics towards adjusting their security policies to genuine hybrid threats from the Russian Federation, a blow to their sovereignty, independence, and integrity with Western security agencies[[4]](applewebdata://3B002A7F-26A5-4E82-AB99-6FCC85AF4BFC" \l "_ftn4). Baltic special services precisely identified these threats in their reports, which confirms how situationally aware they are. This also places Lithuania, Latvia, and Estonia on the list of participants of an unofficial albeit ongoing hybrid conflict between EU/NATO states and Russia.

As a conflict, Russia’s hybrid warfare against European Union (EU) nations and the North Atlantic Alliance, or NATO, is uneasy to define. What awakens research curiosity is the adjective hybrid. It is difficult to find a more dynamically developing concept in security studies than hybrid threat. Linguists define hybrid as “something that is a mixture of different elements, often not matching each other[[5]](applewebdata://3B002A7F-26A5-4E82-AB99-6FCC85AF4BFC" \l "_ftn5).” Thus, in military strategy, hybrid activities are a combination of symmetric and asymmetric war[[6]](applewebdata://3B002A7F-26A5-4E82-AB99-6FCC85AF4BFC" \l "_ftn6). Among the available definitions of a hybrid threat, perhaps the most complex one is that of the European External Action Service, labeling hybrid threats as a combination of “conventional and unconventional, military and non-military activities that can be used in a coordinated manner by state or non-state actors to achieve specific political objectives.” Their diversity consists in the use of tools and tactics “designed to be difficult to detect or attribute,” and “seeking to create confusion to hinder swift and effective decision-making” targeting “critical vulnerabilities.” Hybrid threats “can range from cyberattacks on critical information systems, through the disruption of critical services such as energy supplies or financial services, to the undermining of public trust in government institutions or the deepening of social divisions[[7]](applewebdata://3B002A7F-26A5-4E82-AB99-6FCC85AF4BFC" \l "_ftn7).”

Furthermore, the European Center of Excellence for Combating Hybrid Threats defined hybrid threats as “coordinated and synchronized action, that deliberately targets democratic states’ and institutions systemic vulnerabilities, through a wide range of means.” As the effectiveness depends much on the activities below the thresholds of detection and attribution, any security forces find it either difficult or impossible to deliver an unambiguous defense reaction. Those who present hybrid threats draw the blurred line between concepts like war and peace, ally and enemy, or national or international sphere, both in legal aspects and by their definitions. The top aim of the activity is to influence different forms of decision making at the local, state, or institutional level to favor and gain the agent’s strategic goals while undermining and hurting the target.

A range of components behind hybrid threats is still ready for new additions as the security environment is undergoing dynamic shifts bringing in new facts to the definition.

GEOPOLITICAL FEATURES OF THE BALTIC SEA

With the surface area totaling 415,266 square kilometers, or twice as much as the total area of Belarus, the Baltic Sea consists of a few regions and basins––the Baltic Proper, the Bothnian Sea, the Gulfs of Bothnia, Finland, and Riga. It drains through the Danish straits of the Sound, the Great Belt, and the Little Belt––all of them laying close to the Jutland Peninsula and the Kattegat and Skagerrak straits that separate the Baltic Sea and the North Sea. The Baltic Sea features also some islands being of key importance for geostrategic control of the body of water: Finland’s Åland Islands, Estonia’s Hiiumaa and Saaremaa, Sweden’s Gotland, and Denmark’s Bornholm.

The Baltic Sea is one of the top directions for Russia’s foreign and security policies while also being where Moscow is pursuing its vital interests. In the northern part of the Baltic Sea lies St. Petersburg, a Russian city at the head of the Gulf of Finland, and in the south, there is Kaliningrad Oblast, the country’s military exclave in this part of Europe and its somewhat “window to the West.” This allows Russia to embolden its military presence in the Baltic Sea and have a real impact on the energy security of both countries in the region and the whole European Union.

Running along the Baltic Sea from Vyborg, Russia to Lubmin, Germany, with an annual capacity of 55 billion cubic meters (bcm) of natural gas, the Nord Stream 1 energy link and its sister pipeline, Nord Stream 2, with a similar capacity and set to become operational soon, both bypass Central and Eastern Europe, including the Baltic countries. For the Kremlin, the project is of both political and commercial importance while opening up an alternative route for natural gas flows to Western Europe to go around transit nations like Ukraine[[8]](applewebdata://3B002A7F-26A5-4E82-AB99-6FCC85AF4BFC" \l "_ftn8).

Owing to Cold War-era ties between Lithuania, Latvia, and Estonia on the one hand and Russia on the other, the region is now a battlefield where Moscow is seeking to reconstruct its post-Soviet sphere of influence. So far Russia has revealed its expansive feats there, also by dispatching forces of the Western Military District of the Armed Forces of the Russian Federation, also that of the Baltic Fleet, headquartered in Baltiysk, Kaliningrad, a move that overwhelmed Estonia, Lithuania, and Latvia with a feeling of danger. Besides Russia, amongst the countries enclosing the Baltic Sea are also eight EU member states, of which six belong to the North Atlantic Alliance. Sweden and Finland––both of which are openly seeking to strengthen military ties with both the North Atlantic Alliance and the EU’s Permanent Structured Cooperation (PESCO)––side with the military bloc in the event of a potential conflict. Going further, if a major confrontation arose between Russia and NATO, geopolitically the Baltic Sea might be almost wholly out of control of the Russian Federation[[9]](applewebdata://3B002A7F-26A5-4E82-AB99-6FCC85AF4BFC" \l "_ftn9).

These brief features of the Baltic Sea explain how geopolitically salient the body of water is in an all-out rivalry between Russia and Western nations. Besides, in this report, the geopolitical perspective of the Baltic Sea is fundamental to analyze both current and possible hybrid threats to the security of the Baltic nations, as thoroughly outlined in papers published by their special services.

COMMON HYBRID THREATS OF THE BALTIC STATES

The content of the security and risk assessment reports by the special services of the Baltic states allows us to outline a common denominator for their security environment and draft a universal repertoire of current hybrid threats for the three republics.

1. Russia represents the most serious hybrid threats to the internal security and constitutional order of the Baltic nations. The Kremlin’s belligerent foreign and security policies are linked to the country’s imperialist pursuit to rebuild its position in the Baltic Sea and move its sphere of influence further, to stretch to the Baltics, a move that generates threats to the raison d’Etat of Lithuania, Latvia, and Estonia.  
2. In doing so, Moscow has at its disposal special services––as tools for going ahead with its foreign and security policies towards the Baltic nations to pose the biggest threat possible to both the internal security and constitutional order of Latvia, Lithuania, and Estonia[[10]](applewebdata://3B002A7F-26A5-4E82-AB99-6FCC85AF4BFC" \l "_ftn10). In their reports, all Baltic special services insist on the destructive nature of the activities performed jointly by the Russian intelligence services and their Belarusian peers. Posed by the FSB, GRU, and SVR, hybrid threats to Lithuania, Latvia, and Estonia target a number of areas, notably politics, diplomacy, military, economy, energy, society, and culture. Russian intelligence services’ activities are tracked mainly in Russia, but also the Commonwealth of Independent States, or CIS. Both the FSB and the GRU are actively recruiting Baltic nationals[[11]](applewebdata://3B002A7F-26A5-4E82-AB99-6FCC85AF4BFC" \l "_ftn11). All spying cases disclosed so far in the Baltic States refer to any activities for the benefit of either the Russian Federation or the Republic of Belarus.  
3. In the reports, their authors place in spotlight Moscow’s hybrid actions against the Baltic nations as being part of a broader security and foreign strategy, with the following key goals:  
a) impeding NATO’s expansion toward Russia’s borders, in the Baltic Sea, the Caucasus, and the Balkans;  
b) disintegrating the European Union, undermining its democracy-based legal order, and taking advantage of any situations that bring to the fore chasms between individual bloc members;  
c) promoting international cooperation between Russia and EU states, based on bilateral ties, and not collegial supranational bodies;  
d) building Russia’s image of a “besieged fortress” among European societies by igniting Russophobic moods, a move that integrates and solidifies Russian-speaking communities in these countries, and shifts the perception of Russian foreign policy among members of Russian society.

4. The level of threat from terrorism is low in all three Baltic nations––and so is the likelihood of a terrorist attack. Although other European countries note higher threats levels from right-wing militants, Islamic insurgents, and terror groups, the Baltic countries are now a little interesting target for terrorists. In their reports, security services in Lithuania, Latvia, and Estonia cast a spotlight on a couple of examples where foreign-inspired political and religious extremism came to the fore, with other powers or groups like IS.  
5. The military facet of hybrid threats wholly addressed to the North Atlantic Alliance refers notably to the Baltic nations. In the Russian deterrence strategy, Kremlin senior officials do not resort exclusively to dispatching troops to the Western Military District and carrying out full-scale offensive drills[[12]](applewebdata://3B002A7F-26A5-4E82-AB99-6FCC85AF4BFC" \l "_ftn12). Russia consequently creates perilous situations by holding Baltic Fleet war-gaming exercises right off the coasts of other countries or by repeatedly intruding their airspace.  
6. Latvian, Estonian, and Lithuanian cyberspace is one of the top targets for Russian special services and related agents. In 2007, Estonia became the target of a coordinated cyber attack, the starting point of the cyber war era that made cyberspace a permanent feature of the critical state administration[[13]](applewebdata://3B002A7F-26A5-4E82-AB99-6FCC85AF4BFC" \l "_ftn13). Both VDD and KAPO reported most spying cases among Russian-based hacking groups targeting essentially state and local government institutions and critical infrastructure agencies. In their analyses, VSD and AOTD paid attention to the cyber espionage of Russian intelligence agencies, including the GRU group Sofacy/APT28 and the FSB group Agentbtz/Snake, adding they might employ the fifth-generation (5G) communication technology for cyber espionage. What Lithuania has experienced reveals that Russian special services use the online space to wage disinformation campaigns against defense sectors in the Baltic countries to disgrace them in the eyes of other NATO states. Besides, special services of the Baltic republics pinpointed in their reports a set of intelligence and cyber threats from the People’s Republic of China.  
7. In its report, Latvia’s VDD draws attention to plausible risks originating from what is referred to as Latvian cross-border projects with Russian entities. Latvian municipalities see their cooperation with Russian agencies being part of cross-border projects as risky due to likely espionage perils and their repercussions for the state internal security. Just to cite here an example that involved placing CCTV cameras, an idea put forward by the Pskov region administration, for monitoring natural resources off the Latvian lake districts that the country’s State Security Service eyes as an evident attempt to install spying devices in Latvia to gather intelligence data.

8. According to data from the general population census of 2011, 5.8 percent of Lithuanians were ethnic Russians[[14]](applewebdata://3B002A7F-26A5-4E82-AB99-6FCC85AF4BFC" \l "_ftn14), compared to 26.9 percent (2011) and 24.6 percent[[15]](applewebdata://3B002A7F-26A5-4E82-AB99-6FCC85AF4BFC" \l "_ftn15) (2020) in Latvia and Estonia respectively[[16]](applewebdata://3B002A7F-26A5-4E82-AB99-6FCC85AF4BFC" \l "_ftn16). Russian state agencies seek to integrate Russian-speaking groups in both Latvia and Estonia by using aggressive historical propaganda to promote a positive image of both the Soviet Union and Russia, which poses one of the biggest threats to these states and their constitutional order. Russian diplomats in Riga and Tallinn are also taking active steps to solidify members of the Russian minority, also through agencies like the Russkiy Mir Foundation or Rossotrudnichestvo[[17]](applewebdata://3B002A7F-26A5-4E82-AB99-6FCC85AF4BFC" \l "_ftn17). Efforts to protect ethnic Russians living in the Baltic countries go hand in hand with the Russian hybrid activities that seek to gain the favor of these groups for the Kremlin’s belligerent foreign course and create a positive image of the Russian authorities amongst people in Russia.  
9. Pro-Russian NGOs and public entities take advantage of the benefits of democracy and freedom of speech to produce an accusatory narrative against Latvian and Estonian officials, balking at them over their alleged discriminatory moves against ethnic Russians in both countries. Behind these feats are both Russian diplomats and special services that look to discredit these states in the eyes of other countries around the globe. At a later stage of hybrid activities, Russian-made rhetoric equips Moscow with a comfortable pretext to conceal actions aimed at “protecting an oppressed minority,” a Kremlin solution that played out first in Georgia in 2008, and then in Ukraine in 2014. Any response from Latvian or Estonian officials to these statements is met with accusations of Russophobia, suppression of freedom of speech, human rights abuse, and promoting fascism[[18]](applewebdata://3B002A7F-26A5-4E82-AB99-6FCC85AF4BFC" \l "_ftn18).  
10. Russia is also going ahead with alluring Russian-speaking young people in the Baltic countries to become members of pro-Russian institutions like the Latvian Council of Civic Organisations (LSOP) or the Union of Associations of the Russian Minority in Estonia[[19]](applewebdata://3B002A7F-26A5-4E82-AB99-6FCC85AF4BFC" \l "_ftn19). One more example of Russia’s hybrid activities is an effort to promote an educational offer to encourage young Russian speakers in the Baltic countries to study at universities across Russia. Both Latvia’s VDD and Estonia’s KAPO also warn against Russian efforts to recruit alumni, also those of the Moscow State Institute of International Relations (MGIMO).  
11. Numerous reports by the Baltic special services focus on the Kremlin’s aggressive information policy, historical propaganda, and disinformation campaigns staged by the country’s senior officials[[20]](applewebdata://3B002A7F-26A5-4E82-AB99-6FCC85AF4BFC" \l "_ftn20). Russia’s politics of history has a clear goal: to emphasize the Soviet contribution to the development of the Baltic states while denying their annexation and then occupation. With this narrative, Russia insists on the ties between the former Soviet republics and the Russian Federation, which serves as an attempt to drag them into countries being Moscow’s exclusive sphere of influence. Russia mobilizes historical propaganda messages in the Baltic states to promote its version of history, notably that of World War II[[21]](applewebdata://3B002A7F-26A5-4E82-AB99-6FCC85AF4BFC" \l "_ftn21). In the Russian-made information engineering that constructs the politics of history, the Kremlin tends to resort to the following tools: a) consistent moves to reinterpret past events to make Russia a hero and a liberator, and not an aggressor and occupant, b) erecting new monuments to the Red Army and renovating already existing ones, c) offering (financial) aid to historical events as an opportunity to depict the Russian version of history, d) using media outlets to air television shows aligned with the Russian historical propaganda.  
12. Russia is constantly interfering with political processes in the Baltics by backing political parties being close to the Kremlin’s current political interest. Estonia’s KAPO has drafted a list of pro-Russian political parties and Russian-backed NGOs[[22]](applewebdata://3B002A7F-26A5-4E82-AB99-6FCC85AF4BFC" \l "_ftn22), both serving as a comfortable channel for Russian officials. In Lithuania, special services did not spot any Russian attempt to meddle in the 2019 parliamentary vote yet with its propaganda tools, Moscow waged disinformation campaigns to discard the image of Lithuanian politicians expressing a negative view of Moscow’s current policy.  
13. The Kremlin makes intensive use of public diplomacy in the Baltic nations and other countries to introduce top-down guidelines in its propaganda and information strategies, thus to pose more hybrid threats. One example is Russian-staged events to make the public opinion shift its stance on the annexation of Crimea and give consent to the status quo in the peninsula. Russia’s propaganda apparatus skillfully takes advantage of the fact that foreign officials attend these meetings, portraying this as a sign of international support for Russia’s feats in Crimea, a step that fits into Moscow’s strategic thought and sustains the Kremlin’s narrative of information policy. In the report, Lithuania’s VSD stands firm that such Russian-held conferences open up an opportunity for the country’s special services to recruit new sources that might possibly operate for Russia.  
14. In its hybrid war against the Baltic nations, Russia has a number of legal and institutional tools––like issuing passports or launching repatriation programs. By simplifying legal procedures to acquire Russian citizenship, or passport, Russia reaps a double benefit. First, this comes as an alluring offer for ethnic Russians in Estonia and Lithuania and the whole undertaking increases the share of Russian nationals in the total population of these states. Also, this legitimizes the narrative of the information policy pursued by the Russian propaganda apparatus. Besides, by looking for new citizens outside the country, Russia is trying to tackle the demographic crisis at home[[23]](applewebdata://3B002A7F-26A5-4E82-AB99-6FCC85AF4BFC" \l "_ftn23). Also, through its repatriation program in Estonia, Russian officials sought to convince members of local Russian-speaking groups to return to their “true homeland.” In the report, Estonia’s KAPO even mocked at the failed undertaking.  
15. Economic security is what is of critical importance for the functioning and development of the Baltic countries. Russia consistently balks at infrastructure projects in the Baltic republics––such as Rail Baltica––chiding at them as unprofitable and unsustainable while arguing it develops anti-Russian military infrastructure. Nonetheless, diversifying energy supplies, adding new directions, and expanding the gas pipeline network (Balticconnector) or energy infrastructure projects (EU-wide Connecting Europe Facility) are all vital for the security of the Baltic nations. Also, the electricity systems of the Baltic states and Russia are tightly interconnected and integrated into the BRELL (Belarus, Russia, Estonia, Latvia, and Lithuania) electrical grid that enables Russia to control the frequency regulation and thus put pressure on the Baltic countries[[24]](applewebdata://3B002A7F-26A5-4E82-AB99-6FCC85AF4BFC" \l "_ftn24). The energy sector in the Baltics is still a target of Russian cyber attacks. Russia is sparing no efforts to make the Baltic republics fully reliant on its energy flows while rebuilding the energy security architecture in the Baltic Sea with projects like Nord Stream and its sister gas pipeline Nord Stream 2. Russian feats are also met with resistance from other countries and EU bodies; just to cite here that Germany’s Federal Network Agency rejected the project’s request for a pass from a new EU gas directive[[25]](applewebdata://3B002A7F-26A5-4E82-AB99-6FCC85AF4BFC" \l "_ftn25). One notable example is also the Belarusian nuclear power plant––located some 55 kilometers off Vilnius––that got funds from Russia and violates international safety requirements. In its report, the International Atomic Energy Agency, or IAEA, wrote that the nuclear facility presents a real threat to the Baltic states and whole Central and Eastern Europe.

CONCLUSIONS AND FORECASTS

The analysis of the current hybrid threats to the Baltic states –– as outlined in the special service reports –– makes it possible to deliver an overview of conclusions and forecasts.

1. The Russian Federation poses most hybrid threats to the Baltic nations, a state of affairs that is unlikely to shift anyhow soon. The interference of Russia’s special services into the Baltic republics and their state apparatuses is permanent, wields varied tools, and touches upon multiple sectors. All undertakings in this area come as part of the Kremlin’s foreign and security policy strategy to strengthen its international position, pursue vital national interests, and protect Russian raison d’Etat.  
2.Russia’s annexation of Crimea in 2014 was a trigger that radically changed the perception of the security in the Baltic countries while their senior officials grew aware of a real threat posed by Russia’s expansionist foreign policy and plausible military aggression. Russia’s entering the peninsula also showed the true face of Putin’s imperialist policy and his Pan-Slavic doctrine. Russia’s hybrid activities against the Baltic nations are very perilous if they either go unnoticed or get downplayed before fully identifying them as threats.  
3. Being EU and NATO members and hosting allied forces on their soil, the Baltic countries reduce the risk of a potential conflict or other aggression from the Russian Federation. But with the growth in intensity, scale, variety, and multiple nature of hybrid threats Russia continues to pose to the Baltic countries, there rises the future possibility of a hybrid war into conventional aggression and a repeat of the Crimea scenario throughout the whole Baltics or in just one of them, for instance in Latvia.

#### Goes nuclear.

Hal Brands 19, Hal Brands is a senior fellow at the American Enterprise Institute, where he studies US foreign policy and defense strategy. Concurrently, Dr. Brands is the Henry A. Kissinger Distinguished Professor of Global Affairs at the Johns Hopkins School of Advanced International Studies (SAIS). He is also a columnist for Bloomberg Opinion, November 2019, "How Russia Could Force a Nuclear War in the Baltics," https://www.aei.org/op-eds/how-russia-could-force-a-nuclear-war-in-the-baltics/ //AShah

Would the US fight a nuclear war to save Estonia? The question would probably strike most Americans as absurd. Certainly, almost no one was thinking about such a prospect when NATO expanded to include the Baltic states back in 2004.

Yet a series of reports by the nonpartisan RAND Corporation shows that the possibility of nuclear escalation in a conflict between the North Atlantic Treaty Organization and Russia over the Baltic region is higher than one might imagine. The best way of averting it? Invest more in the alliance’s conventional defense.

There was a time when it seemed quite normal to risk nuclear war over the sanctity of European frontiers. During the Cold War, NATO was outnumbered by Warsaw Pact forces, and it would have had great difficulty stopping a Soviet attack with conventional weapons. From the moment it was formed, NATO relied on the threat of nuclear escalation — whether rapid and spasmodic, or gradual and controlled — to maintain deterrence. American thinkers developed elaborate models and theories of deterrence. US and NATO forces regularly carried out exercises simulating the resort to nuclear weapons to make this strategy credible.

After the Cold War ended, the US and its allies had the luxury of thinking less about nuclear deterrence and war-fighting. Tensions with Russia receded and nuclear strategy came to seem like a relic of a bygone era. Yet today, with Russia rising again as a military threat, the grim logic of nuclear statecraft is returning.

The spike in tensions between Russia and the West over the past half-decade has revealed a basic problem: NATO doesn’t have the capability to prevent Russian forces from quickly overrunning Estonia, Latvia and Lithuania. Russian invaders would be at the gates of the Baltic capitals in two to three days; existing NATO forces in the region would be destroyed or swept aside. NATO could respond by mobilizing for a longer war to liberate the Baltic countries, but this would require a bloody, dangerous military campaign. Critically, that campaign would require striking targets — such as air defense systems — located within Russia itself, as well as suppressing Russian artillery, short-range missiles and other capabilities within the Kaliningrad enclave, which is situated behind NATO’s front lines.

Moreover, this sort of NATO counteroffensive is precisely the situation Russian nuclear doctrine seems meant to avert. Russian officials understand that their country would lose a long war against NATO. They are particularly alarmed at the possibility of NATO using its unmatched military capabilities to conduct conventional strikes within Russian borders. So the Kremlin has signaled that it might carry out limited nuclear strikes — perhaps a “demonstration strike” somewhere in the Atlantic, or against NATO forces in the theater — to force the alliance to make peace on Moscow’s terms. This concept is known as “escalate to de-escalate,” and there is a growing body of evidence that the Russians are serious about it.

A NATO-Russia war could thus go nuclear if Russia “escalates” to preserve the gains it has won early in the conflict. It could also go nuclear in a second, if somewhat less likely, way: If the U.S. and NATO initiate their own limited nuclear strikes against Russian forces to prevent Moscow from overrunning the Baltic allies in the first place. And even the limited use of nuclear weapons raises the question of further escalation: Would crossing the nuclear threshold lead, through deliberate choice or miscalculation, to a general nuclear war involving intercontinental ballistic missiles, strategic bombers and apocalyptic destruction?

## Cyber Attacks

#### Lithuania facing onslaught of intense Russian hacks

Manthorpe 6-28 (Rowland, studied History at Cambridge and Political Theory at the London School of Economics, and has been awarded the Ben Pimlott Prize for Political Writing by the Guardian and The Fabian Society. Rowland is Technology correspondent, reporting on the many areas tech is transforming lives. “Could the Russian cyber attack on Lithuania draw a military response from NATO?”, https://news.sky.com/story/could-the-russian-cyber-attack-on-lithuania-draw-a-military-response-from-nato-12641986)LR

**A NATO member is under attack.** The NATO member in question is the Baltic state of **Lithuania**, which was **targeted on Monday by Russian hackers.** According to the hackers, the attack is still going on. Transport and media websites have been hit, as have the websites of various state institutions such as the Lithuanian tax service, which had to pause its operations yesterday. A Russian hacker group known as Killnet claimed responsibility for the attacks, claiming on its Telegram channel that the attack was retaliation for Lithuania's decision to stop the transit of some goods to the Russian territory of Kaliningrad on the Baltic coast. The politics of this situation are extremely complicated. Kaliningrad is Russian-owned, but it isn't connected to the main body of Russia - it's a small piece of Russia surrounded by NATO countries. The Lithuanian government says it is simply enforcing European Union sanctions on goods, but Russia has responded with outrage, saying it is being stopped from accessing its sovereign territory**. Russia promised to respond** in a way **that would "have a serious negative impact on the population of Lithuania"**. Then, a **few days later, came this cyber attack**. Does that mean Russia attacked a NATO member? Not so fast. For a start, the group that claimed responsibility denies any connection to the Russian state, saying it is "not affiliated with any law enforcement authorities". The Russian government has long used third-party criminal groups to conduct hacks and cyber attacks, so it would not come as a surprise if it was involved. Nevertheless, on the surface at least, its hands are clean. Then there's the nature of the attack. Reports so far suggest that it's a distributed denial of service (DDoS) attack, a crude attack which involves throwing huge amounts of traffic at a website until it is forced offline. The attack has been described as "massive", which is technically true, because in order to work a DDoS attack has to be large, but that doesn't mean it will have a massive effect. DDoS attacks are so common that most websites nowadays have protection against them as standard. Even if an attack does work, it won't steal any data. It's a blunt force instrument, little more. Yet that does not mean we aren't moving towards that point, nor that a cyber attack cannot lead us there. Another way in which cyber attacks are different to physical attacks is that once they are started they can spiral out of control. Unlike a bomb or a bullet, a virus can spread in ways that even its makers don't intend. Almost exactly five years ago, the costliest ever cyber attack was launched: a malware attack called Not Petya. It is believed to have begun when Russian operatives infected a small piece of Ukrainian accounting software, intending to disrupt Ukrainian businesses. But from there it spread to companies around the world, including shipping giant Maersk and food conglomerate Mondelez. By the time it was done, Not Petya had caused $10bn in estimated damages.

#### Draws in NATO and the US

Zemelyte 6-27 (Beatrice, BA in Administration, Human Resources, and Marketing at University of Vermon, interviewing Agnia Grigas - Dr. Agnia Grigas is an energy and political risk expert. She specializes in energy and foreign policy of the U.S. and Eurasia including Europe, Russia, China, the states of the former Soviet Union, and the Baltic States. She has fifteen years of experience as a business development and political risk advisor to corporations and government agencies. She is an author of three critically acclaimed books The New Geopolitics of Gas (Harvard University Press, 2017), Beyond Crimea: The New Russian Empire (Yale University Press, 2016), and The Politics of Energy and Memory Between the Baltic States and Russia (Ashgate 2013). Dr. Grigas graduated cum laude with a BA in economics and political science from Columbia University, New York, NY and earned her Master’s and Doctorate in international relations from the University of Oxford, UK where she is an alumna of St Antony’s and Brasenose colleges. “Kaliningrad standoff could reveal if Russia wants to ‘escalate’”, https://www.aljazeera.com/news/2022/6/24/achilles-heel-of-nato-tensions-amid-kaliningrads-transit-ban)LR

Al Jazeera: Russia has said Lithuanian citizens will “feel the pain” over Kaliningrad. How might Moscow respond? Grigas: Russia could enact its own sanctions on the sale of goods to Lithuania. The key Russian exports are oil and gas, and electricity, and Lithuania has already made a decision much earlier before this conflict, that it will not be purchasing any Russian energy sources. There could be a question of fertilisers and other elements but there is already a broad blanket of European sanctions against Russian goods. I view Russia’s statements more as threats and posturing for the Russian domestic audience because a lot of [Russian President Vladimir] Putin’s statements tend to be aimed to show the resolve and the strength of the Kremlin, rather than necessarily specifying any sort of actions they would take or for the external audience. What is concerning is that Russia used or the Kremlin use the terms that Lithuania has enacted a blockade, either the word choice is important, because blockade could be perceived as a military already action, and therefore, Russia could try to, you know, justify some sort of [military action], as well.” Al Jazeera: How do you think the Kaliningrad situation can impact the war in Ukraine? Grigas: I think this situation in Kaliningrad will show whether Russia is willing to escalate further this conflict against the West, the European Union and NATO. Al Jazeera: The United States has said that it will stand behind Lithuania and its NATO commitments to defend it … Grigas: NATO, the United States and European Union countries have been very cautious not to get involved in this war. There’s a real fear of potential escalation of conflict with Russia directly because one, Russia remains a nuclear state. Second, because of the fact that it’s controlled essentially by a single man with a very small circle of advisers, who has essentially a free hand to take whatever decisions he may wish. Al Jazeera: Lithuania and Russia already had weak diplomatic relations, and the war in Ukraine has worsened them. How will their ties be affected by the ban? Grigas: Lithuania has been a very vocal supporter of Ukraine since the very start of the war this February and, frankly, since Russia’s occupation of Crimea [in 2014] and the initial invasion of the Donbas. Earlier this summer, Russia and Duma deputies were discussing whether they should revoke Lithuania’s independence that was agreed to by the Soviet Union in 1991. This is part of kind of a broader package of the Kremlin’s threats on a smaller neighbouring country. I don’t think Lithuanian-Russian relations will improve in the near future. Frankly, European and Russian relations will not improve in the near future, nor will NATO and Russian relations, particularly as long as the ongoing war in Ukraine continues.

### Critical Infrastructure Scenario

#### Russian and Chinese cyber-attacks on critical infrastructure is coming now – laundry list of impacts – NATO cohesion, CI, trust in institutions, Saudi energy.

Dupay et al 21 [Dr Arnold C. Dupuy is a Science Applications International Corporation (SAIC) employee and Chair of the NATO Science and Technology Organization’s program to study hybrid warfare. Dr Dan Nussbaum is a faculty member at the Naval Postgraduate School, the Chair of the NPS Energy Academic Group, and is the Mentor of the NATO Science and Technology Organization’s program to study hybrid warfare. Vytautas Butrimas works in the area of industrial cybersecurity for the NATO Energy Security Centre of Excellence. Alkman Granitsas is a communications consultant at Kyklos Associates with a focus on public policy issues. 1-13-2021, "NATO Review", NATO Review, https://www.nato.int/docu/review/articles/2021/01/13/energy-security-in-the-era-of-hybrid-warfare/index.html, DOA: 7-20-2022 //ArchanSen]

Hybrid warfare is roughly defined as ‘grey area’ warfare, which often exists just beneath the threshold of armed conflict. It is designed to erode public confidence in civil society and democratic foundations, primarily through cyber attacks on critical infrastructure, including energy, or targeted disinformation methods. In this regard, it poses a potential threat to sovereignty, as it gives nations, terrorist organisations and criminal actors relative anonymity via a low-cost, high-yield method to influence the politics and policies of other states.

Russia is one of the most active perpetrators of hybrid warfare and implemented it most effectively in its 2014 illegal annexation of Crimea. The Kremlin continues to use it today, notably in some countries to realise desired political outcomes such as undermining pro-Western governments, dividing and weakening the NATO Alliance, or advancing its own economic interests. China too has recently engaged in cyber attacks and disinformation campaigns aimed at NATO Allies and poses a grave risk to critical infrastructure, including energy infrastructure, as highlighted in the recent NATO 2030 experts’ report.

Ultimately, hybrid warfare challenges to the energy sector have the potential to disrupt the NATO’s political and military effectiveness and cohesion. It will take time and effort to counter these threats, if the Alliance is to address dependencies among its members and act as a platform to build a common picture of complex operational risk and vulnerabilities.

Energy sector increasingly targeted

The use of hybrid warfare is growing. The past decade has seen a dramatic increase in hybrid threats worldwide: from cyber attacks to disinformation campaigns to covert military operations. Threats are becoming more frequent, complex, destructive and coercive. The broader economic and security ramifications of hybrid warfare are evident, especially when applied to the energy sector.

Russia has deployed a range of hybrid threats against the energy assets, policies or supplies of NATO Allies, as well as other countries. It has used political and economic leverage, combined with disinformation campaigns, against Bulgaria and Romania to undermine efforts to reduce their dependence on Russian energy sources. Supply disruptions have been used in the past as well, most famously in the case of Ukraine in 2009, the Baltic states before that and, more recently, against Bulgaria.

Russia has also used its economic clout, combined with political influence, to advance its energy agenda, in Hungary, where the expansion of the Paks Nuclear Power Plant is now underway using Russian energy technology. Likewise, in Germany, Russia has used its commercial and political ties, as well as other suspected malign influence, to advance the controversial €12 billion Nord Stream II pipeline, now nearing completion. Moreover, in 2020, a suspected Russian group, Berserk Bear APT, launched cyber attacks against German energy companies, and has been implicated in previous cyber attacks against German utilities in 2018.

Russian-backed cyber attacks against energy assets have also been identified in a number of other Alliance members, including Poland, Turkey, the United Kingdom and the United States. In some instances, those cyber campaigns have run concurrent with other hybrid threats against energy assets, like malign influence efforts and natural gas supply cutbacks. Taken together, it is clear that – over the past decade and with increasing vigour – Russia has been pursuing a concerted hybrid campaign aimed at undermining the Alliance’s energy security.

Over the same period, among NATO’s partner countries, Russia’s hybrid campaign has been most evident in Ukraine, combining supply disruptions, cyber attacks, economic and political influence, and disinformation efforts to undermine the country’s energy security and sow political instability. The most disruptive effort was Russia’s 2009 interruption of natural gas supplies, but the attacks have continued and become increasingly complex and coercive.

A notable example is the December 2015 Black Energy cyber attack on the western Ukrainian power station, which shut down power for nearly a quarter million residents over a six hour period. This was followed, a year later, with a more sophisticated attack on the power grid supplying electricity to the capital, Kyiv, using CrashOverride/Industroyer malware. While of shorter duration and scope than the previous attack, the effort was far more sinister: it was aimed at compromising electrical safety relays, which are used to protect bulk power equipment. Had it not been detected by analysts, the final attack phase could have led to physical destruction of expensive and difficult-to-replace equipment beyond briefly disrupting power supplies.

Beyond the Euro-Atlantic area, Iran and other suspected states are currently waging a complex hybrid campaign against Saudi Arabia’s energy assets. This campaign may be illustrative of the future of hybrid warfare, particularly in the domain of energy security. Through both covert and overt military operations, and the use of proxy forces, Iran has repeatedly disrupted or otherwise struck Saudi energy infrastructure.

The possible collusion of hostile actors in the ongoing Iranian campaign against Saudi Arabia is of particular concern and may have consequences for NATO Allies. Specifically, the 2017 cyber attack on the Petro Rabigh complex, which resulted in a costly shutdown and forensic clean-up of the facility and very nearly resulted in an uncontrolled gas release and explosion. Despite initial speculation that Iran was uniquely responsible for the dangerous Triton malware used in the attack, the United States has since concluded that the malware was developed by Russia and imposed sanctions on the research institution connected with its development. The malware has also been implicated in attacks on energy companies in the United States.

Other suspected measures in Iran’s campaign include two drone strikes by Iran’s Houthi allies on Saudi refineries, covert attacks on two Saudi registered oil tankers in the Persian Gulf and, most recently, attacks on two foreign-flagged tankers at Saudi ports on the Red Sea. Notably, the drone strike on the Saudi Aramco Abqaiq refinery in late 2019, which was claimed by Houthi forces, provided Iran with deniability and helped expose air defence weaknesses in Saudi Arabia.

#### CI – extinction.

Delacourt 22 [[Ted P. Delacourt](https://www.hstoday.us/author/tdelacourt/) 02-01-2022, "Cyberattacks on Critical Infrastructure as the New WMD", Hstoday, https://www.hstoday.us/featured/cyberattacks-on-critical-infrastructure-as-the-new-wmd/, DOA: 7-20-2022 //ArchanSen]

Should the acronym WMD, which stands for “Weapons of Mass Destruction,” be updated to “Weapons of Mass Disruption?” I think it is a timely question in this Digital Age as we connect and integrate billions of new digital devices into our lives and business processes and when a cyber-attack against one supply chain provider can lead to cascading effects on entire communities across the globe. Cyberattacks on Critical Infrastructure (CI) can cause mass economic and societal impacts. Fewer strategies than cyber-attacks can offer better plausible deniability and can cause greater anxiety and instability to our society than targeting the systems and networks that enable our day-to-day activities. Consider that 20 years ago terrorists killed 3,000 Americans and disrupted the entire U.S. and global economies with only four planes. Given the growth and ubiquity of technology today we must consider how the exponential growth of cyberattacks on CI might be similarly leveraged by adversaries and criminal actors as Weapons of Mass Disruption, the new WMD.[1]

Cyberattacks take many forms, often progressing through multiple phases as they escalate in severity. Malicious actors often initiate a network intrusion through phishing campaigns or the purchase of compromised user credentials on the dark web. What begins as the hijack of a single user profile expands in severity. Intruders move laterally across internal systems, conducting surveillance and gathering intelligence on network environments before escalating to data theft, service disruptions, and ransomware extortion.

The goals of these actors may be both strategic and economic in nature, and targets may be government and/or the private sector. Cyberattacks perpetrated on CI elements develop into the new WMD when the intended and unintended consequences cause widespread damage and societal impacts. A disruption of essential services, even if brief, can occupy significant civilian and military resources in a region or entire country.[2]

## AT: MAD/A5

#### Article 5 and MAD fail.

Klein et al. 19 [Colonel Robert M. Klein, Senior Military Fellow in the Center for Strategic Research (CSR), Institute for National Strategic Studies, at the National Defense University; Lieutenant Commander Stefan Lundqvist, Ph.D., Researcher and Faculty Board Member at the Swedish Defence University (SEDU); Colonel Ed Sumangil, USAF, Senior Military Fellow in CSR; Ulrica Pettersson, Ph.D., assigned to SEDU, Adjunct Faculty Member at Joint Special Operations University; 11-2019; "Baltics Left of Bang: The Role of NATO with Partners in Denial-Based Deterrence"; No Publication; https://inss.ndu.edu/Portals/68/Documents/stratforum/SF-301.pdf; KL]

Deterrence Options

Political science literature distinguishes between two basic ways to deter an opponent.10 Deterrence through punishment threatens to impose severe costs on an enemy if an attack occurs. Punishment deters by the risk it places against high-value Russian assets, but it also expands the conflict. The Alliance may not choose to defend its interests directly at the point of attack, where Russia has chosen the time and ground of attack. Rather than accept battle where it is least prepared or under the most adverse terrain, NATO may strike at more vulnerable and valuable targets in order to threaten a more opportune place, either a vulnerability or a gap in Russia’s defenses. Punishment is not necessarily connected to the direct defense of the contested space but could include wider penalties—such as nuclear escalation or expanding the geographic boundaries of the conflict—that would raise the costs for an aggressor. Deterrence through punishment is one option to influence the enemy’s cost-benefit analysis. On the other hand, denial-based deterrence seeks to deter an aggressor by making the chance of a successful attack improbable, cost-prohibitive, or untenable. Deterrence through punishment is inherently offensive, while denial-based deterrence is defensive in nature.11

Deterring Russian aggression in the Baltics short of military hostilities, or “left of bang,” is a political problem in which U.S. and NATO militaries are but one component. Because of the presence of nuclear weapons on both sides, the overriding consideration regarding any confrontation between NATO and Russia over the Baltics would require managing both vertical and horizontal escalation. The Alliance must construct any deterrent strategy around that premise so that any actions taken in the deterrence phase naturally mesh with a construct for management of escalation up to and including armed conflict, should that occur. A key concept of deliberate escalation is indicating to an enemy that the costs will outweigh the potential benefits gained through continued particular actions.

In the case of the Baltics, however, punishment-based deterrence may lack credibility if Russia perceives that NATO lacks the capability or resolve to carry out such a retaliatory threat—conventional or nuclear. Another weakness of punishment-based deterrence is the asymmetry of stakes between parties. With the proximity of the Baltics to its borders, Russia may be willing to bear greater costs and, therefore, feel itself less vulnerable to threats of punishment if it perceives Russian stakes are high and NATO’s stakes are low.12 Finally, as former As sistant Secretary of State Wess Mitchell observes, should Russia gain the Baltic states through a fait accompli, “punishment quickly morphs into compellence—not just dissuading an enemy but dislodging him and forcing a withdrawal from his limited, stealthy conquest.”13 In order to deter an adversary, the Alliance needs to both possess a capability and have the willingness to use it. Consequently, at its logical extremes, punishment could entail the threat of a NATO counterattack, possibly using ground forces staged in Poland via a push through the Suwalki Gap, which would be time consuming to prepare, militarily costly, and carry significant operational and escalatory risks given the likelihood of extending the conflict to Belarus, Kaliningrad, or even Russia proper. Such a scenario, a ground war in the Baltics between NATO and Moscow, would play to Russian strengths and represents a poor proposition for successful defense of the Baltic states.14 Additionally, Russia’s tactical nuclear doctrine of “escalate-to-deescalate” further erodes deterrence by punishment, assuming the United States and its Allies would be reluctant to use nuclear weapons in kind, both out of an uncertainty about escalation management and a modern-day aversion to high casualties.15

## Cyber---AT: Alt Cause

#### No natural hazards in the Baltics.

Juurvee 22 [Ivo Juurvee, Head of Security & Resilience Programme and Research Fellow at the International Centre For Defence and Security; 2022; "Energy and Critical Infrastructure Security: The Case of the Baltic States"; *Hybrid Threats in Baltics and Taiwan: Commonalities, Risks and Lessons for Small Democracies*; https://www.baltdefcol.org/files/files/publications/Hybrid%20Threats\_LIIA.pdf#page=38; KL]

With the highest peak of only 318 m over sea level, the Baltic states are flat. The countries are not situated in a seismically active region, neither are they threatened by tsunamis or tornados. However, there are still some natural hazards to critical infrastructure and power supply, mostly caused by the cold or stormy Northern European weather. While floods are usually not dangerous and at some places even considered to be a tourist attraction (Pamarys region  in Lithuania and Soomaa in Estonia), the autumn and winter storms can be more dangerous, especially in Estonia. While short term power cuts and the inaccessibility of roads are usual and appear every year with both the authorities and population well prepared for them, from time to time things get more extreme. In December 2010, almost 600 people were stuck in their cars in the snowstorm on Tallinn– Narva road. One of the main roads of the country was blocked for a day and it was a close call that nobody froze to death. Rough weather in Southern Estonia in December 2019 disrupted the power supply of over 50  000 clients and took days to fix. However, although events like these do happen in the Baltic states, they do not have disastrous effects on infrastructure.13

## Cyber---Baltic War

#### Disads are thumped, but war is still likely. NATO cohesion is key.

FT 22 [The Editorial Board of *Financial Times*; 6-27-2022; "Nato must show it is serious about defending its eastern flank"; *Financial Times*; https://www.ft.com/content/8c45da56-e8af-465b-882a-7fc8455a03d5; KL]

Would Vladimir Putin send Russian troops into one of the Baltic states, knowing this would trigger a direct war with Nato? There is no room for complacency; until Russian tanks rolled across Ukraine’s borders on February 24, that too seemed unthinkable. EU and G7 summits in the past few days have committed to stepping up support to Ukraine — which on Monday suffered a horrific missile attack on a shopping centre in Kremenchuk — and to tightening sanctions that have sapped Russia’s economy and put it on course for its first debt default since 1998. Tuesday’s Nato summit in Madrid is a moment for the alliance to demonstrate that it comprehends the magnitude of the threat from the Kremlin — and is ready and equipped to defend against any Russian attempt to go beyond Ukraine and attack Nato’s eastern flank.

Estonia’s prime minister Kaja Kallas warned last week her country would be “wiped off the map” under existing Nato plans that would allow the Baltic republics to be overrun in any Russian invasion, before liberating them after 180 days. Even as she spoke, Moscow was threatening “serious negative” consequences to nearby Lithuania after it barred rail transfer of some goods to the Russian exclave of Kaliningrad — though Vilnius said it was merely applying EU sanctions.

Brussels has attempted to calm the tensions. But the incident underlined the sensitivity of the three Baltic states, occupied by the Soviet Union for half a century — and of the Suwałki Gap, the Polish-Lithuanian border strip between Kaliningrad and Belarus, which, if seized by Russia, could cut off the Baltics from Nato.

Plans to be endorsed by Nato in Madrid go less far than Kallas would have liked. They are pivotal nonetheless. The alliance is rightly moving from a “tripwire” concept, under which Nato stationed about 1,000 foreign troops in each country to deter invasion, to a focus on a full and rapid defence of allied territory. Nato will put several thousand troops in each Baltic state, and expand its rapid reaction force from 40,000 to 300,000, ready to start deploying to specific eastern locations — where they will have trained and completed exercises — within hours of an attack. More heavy weapons, logistics and command-and-control assets will be pre-positioned.

This is in part a reversion to the Cold War-era model, when Nato’s top commander knew exactly which forces were on standby, where, and how quickly they could move. Yet many lessons on deterrence, defence and signalling have been forgotten in the three decades since, and must be relearnt.

It is vital, too, to put in place the monitoring, decision-making and logistics needed to enable forces to be swiftly deployed. So is the funding to ensure adequate levels of readiness are constantly maintained. Nine Nato states now meet the target of spending 2 per cent of economic output on defence; 19 more have “clear plans” to do so by 2024. Yet Western allies have made too many declarations since Russia seized Crimea and parts of east Ukraine in 2014, without proper implementation. The priority is to convince Putin — who some officials fear does not think Nato’s defence of the Baltics is credible — that the alliance’s security guarantees apply equally across all members.

The alliance could have presented a more compelling image of solidarity, however, were Turkey not still blocking membership for Finland and Sweden over their links to Kurdish separatists. Appearances matter. The north Atlantic alliance is, belatedly, adopting a strategic concept that recognises Russia as the “most significant and direct threat” to its security. But, as in the Cold War, Nato allies must be ready once more to put serious effort and expense into preparing for something it hopes will never happen — with the aim of making sure that it never does.

## Impact---Nuclear

#### Goes nuclear. Quantity of nukes and escalate-to-deescalate make it likely.

NSNWs = non-strategic nuclear weapons

TNWs = tactical nuclear weapons

Brookes 22 [Dr. Peter Brookes, Heritage Foundation senior fellow and a former U.S. Deputy Assistant Secretary of Defense; 3-5-2022; "Russia’s Small Nukes are a Big Problem for European Security"; Monitor Strategic; https://ispaim.mapn.ro/webroot/fileslib/upload/files/Monitor%20Strategic/ms122022.pdf#page=47; KL]

With Russia’s ongoing war in Ukraine, now is a good time to take note of a little-spoken-of, but glaring, imbalance between America’s and Russia’s nuclear arsenals—and how it could affect stability in Europe and the interests of the United States and those of its European allies and partners.

If asked, many Americans and Europeans probably believe that the United States and Russia are pretty evenly matched in terms of the number of nuclear weapons both sides have in their arsenals. While their beliefs are entirely understandable, they are not completely correct

Under the 2010 bilateral New Strategic Arms Reduction Treaty—also known as New START—the United States and Russia have a similar number of deployed strategic (i.e., high-yield and long-range) nuclear weapons: 1,550 deployed nuclear warheads each.1 But not all of Washington’s or Moscow’s nuclear weapons are covered by New START.

Indeed, Russia has nearly a 10:1 advantage over the United States and NATO in non-strategic (i.e., low-yield and short-range) nuclear weapons (NSNWs).2

Assessments based on open sources estimate that Russia has about 2,000 NSNWs. It is similarly assessed that the United States and NATO have about 200 NSNWs in their arsenal.3 It is postulated that half of those U.S.-NATO weapons are located in the United States and half are based in Europe as part of NATO’s nuclear forces.4

While capable of significant destruction, these tactical nuclear weapons are lower in yield – or explosive power – and are meant for use on the battlefield against military installations or troop and equipment concentrations as opposed for use against counterforce or countervalue targets such as ICBM missile fields, command and control nodes, and or population centers (e.g., cities).

It is believed that Russia can deploy these weapons on multiple tactical systems including dual-capable short-range or theater ballistic missiles, torpedoes, and anti-ship missiles.5 Indeed, it is expected that Russia’s new hypersonic weapons may be dual-capable (i.e., conventional or nuclear armed) as well.6

Major nuclear weapons states, including Russia, have said that a nuclear war could never be won and therefore should never be fought. However, there are deep concerns among policy makers and security analysts outside Russia about whether Moscow fully embraces that idea or if it is just convenient diplomatic rhetoric.

Also of increasing concern is a Russian military doctrine associated with battlefield nuclear weapons known as “escalate to deescalate.” This topic is of particularly interest right now with the war in Ukraine ongoing since late February 2022. According to the 2018 U.S. Nuclear Posture Review (NPR):

“Russia considers the United States and the North Atlantic Treaty Organization (NATO) to be the principal threats to its contemporary geopolitical ambitions. Russian strategy and doctrine emphasize the potential coercive and military uses of nuclear weapons. It mistakenly assesses that the threat of nuclear escalation or actual first use of nuclear weapons would serve to “de-escalate” a conflict on terms favorable to Russia. These mistaken perceptions increase the prospect for dangerous miscalculation and escalation.”7

The NPR further asserts that:

“Moscow threatens and exercises limited nuclear first use, suggesting a mistaken expectation that coercive nuclear threats or limited first use could paralyze the United States and NATO and thereby end a conflict on terms favorable to Russia. Some in the United States refer to this as Russia’s “escalate to de-escalate” doctrine. “Deescalation” in this sense follows from Moscow’s mistaken assumption of Western capitulation on terms favorable to Moscow.”8

Though the Russians seemingly refute the existence of this doctrine by its American name at least, some sources assert that the policy may actually have been developed in the late 1990s, when now-Russian President Vladimir Putin was chairman of the Russian National Security Council under President Boris Yeltsin.9

The idea behind escalate to deescalate is that Russia might employ one tactical nuclear weapon (or more) during a conventional conflict with NATO forces for the purposes of preventing a defeat, consolidating territorial gains, or even freezing a conflict in place without the prospect of further fighting.

Indeed, because of the large, nearly 10:1 disparity between the number of Russian and U.S. tactical nuclear weapons, Moscow may think a nuclear response from NATO is not a credible threat due to Russia’s asymmetric advantage. Other factors may also play a role in Russian calculations, including a perception that NATO’s large membership would have difficulty finding a political-military consensus on an appropriate response, including a nuclear option.

An example of the potential use of this Russian nuclear doctrine in a hypothetical scenario might be helpful here:

Moscow attacks one—or all—of the Baltic States with its conventional forces to establish control over some, or all, of these nations’ territory, returning them to Russia’s control as they were in the Soviet era. Invoking Article V, NATO responds with conventional forces to protect and restore the sovereignty of these three allied states.

Concerned about the inferiority of its conventional forces in this fight against the allied powers, Moscow then contemplates exploding a low-yield tactical nuclear weapon somewhere in theater as a warning of Russia’s potential escalation from the conventional to the nuclear domain of warfare, including the potential future use of high-yield, strategic nuclear weapons.

In Moscow’s eyes, perhaps NATO will become concerned about the possible escalation of the fighting from the conventional to the nuclear—especially Russia’s potential use of more powerful nuclear weapons against European and American cities. In response, NATO may consider pausing its counteroffensive against Russian forces in the Baltics.

Indeed, Moscow may misperceive that if NATO does not have sufficient tactical nuclear weapon capabilities to respond in kind, it would be inclined to seek de-escalation rather than launch a strategic nuclear weapon at Russia and risk moving further up the escalation ladder—a response that could lead to all-out nuclear war.

Using its tactical nuclear weapon advantage over NATO and having strategic nuclear parity with Washington, Moscow could threaten additional low-yield nuclear strikes unless fighting ends on Russia’s terms. Ideally for Moscow, NATO might decide that there is no good option available to respond and chooses to cease hostilities, locking in Moscow’s ill-gotten gains in the Baltics.

With these political-military calculations in mind, Russia takes a chance on the expected NATO response and explodes a 10-kiloton tactical nuclear weapon near or in the European theater. As a result, nuclear deterrence fails for the first time in history not due to the use of strategic nuclear weapons that so many people are aware of, but the imbalance of battlefield nuclear weapons between NATO and Russia.

#### Baltics hybrid war goes nuclear.

Kühn 18 [Ulrich Kühn, nonresident scholar at the Carnegie Endowment for International Peace, and a senior research associate at the Vienna Center for Disarmament and Non-Proliferation (VCDNP)/James Martin Center for Nonproliferation Studies, based in Vienna, Austria. Previously, he was a Stanton Nuclear Security Fellow with Carnegie’s Nuclear Policy Program, and a fellow with the Institute for Peace Research and Security Policy at the University of Hamburg (IFSH). He holds a PhD (summa cum laude) in political sciences from Hamburg University, an MA in Peace Research and Security Policy from Hamburg University, and a Magister Artium in medieval and newer history as well as German literature from the Rheinische Friedrich Wilhelms University Bonn. His current research focuses on NATO-Russian relations, transatlantic security, nuclear and conventional deterrence and arms control, and the proceedings of the OSCE. Kühn worked for the German Federal Foreign Office and was awarded United Nations Fellow on Disarmament in 2011. He is the founder and a permanent member of the trilateral Deep Cuts Commission and an alumnus of the ZEIT Foundation Ebelin und Gerd Bucerius; 3-28-2018; “Preventing Escalation in the Baltics: Summary”; *Preventing Escalation in the Baltics: A NATO Playbook*, pages 1-5, Carnegie Endowment for International Peace; https://carnegieendowment.org/files/Kuhn\_Baltics\_INT\_final\_WEB.pdf; KL]

SUMMARY

AMID THE ROLLOUT of the February 2018 U.S. Nuclear Posture Review, security analysts have understandably focused much attention on its implications for the U.S. nuclear arsenal, intra-alliance ties with key North Atlantic Treaty Organization (NATO) partners, and Washington’s icy relations with Moscow. But nuclear deterrence only partially addresses NATO members’ shared concerns about Russian behavior, especially in light of Moscow’s growing propensity to undermine the alliance with nonkinetic operations and other tactics that nuclear warheads cannot easily deter.

The risk of escalation sparking a wider conflict—deliberately, inadvertently, or accidentally—between Russia and NATO is dangerously high. This is particularly the case in the Baltics, a region that would be difficult for NATO to defend because the military balance there very much favors Russia; moreover, Moscow could instigate unrest among the Russian minorities living there. To mitigate these risks and remain united, NATO members must complement deterrence with resilience and risk-reduction measures better tailored to addressing Russian behavior below the threshold of outright conventional and nuclear conflict.

THE CHALLENGE RUSSIA POSES

To keep the West out of the non-NATO former Soviet republics, Moscow has developed new-generation warfare, a coercive strategy that combines traditional conventional and nuclear military capabilities with nonkinetic operations such as cyberattacks, propaganda, and disinformation.

NATO members have different views of Russia’s intentions toward the alliance and how to respond. In the wake of the Ukraine crisis, some allies fear that Moscow could use military force against NATO, particularly the Baltic states. They urge the alliance to do more, militarily, to deter Russia and to reassure its easternmost members. They fear that NATO’s current response—including, most importantly, the deployment of a trip wire force of four multinational battalions, the Enhanced Forward Presence (EFP), to the three Baltic states and Poland—might not be enough to deter deliberate Russian escalation. Others are rather skeptical that Moscow presents an immediate military threat and caution against unnecessarily raising tensions further. Instead of deploying additional forces, they want NATO to focus on increasing the resilience of member states against Russian nonkinetic operations and to engage in a serious security dialogue with Russia, reducing the risks of inadvertent and accidental escalation.

Both approaches could create the risk of miscalculation and, perhaps, escalation. If NATO underestimates the threat Russia poses, the alliance may give Moscow reason to test its resolve—perhaps even by using military force. Conversely, if NATO overestimates the threat emanating from Russia, its well-intentioned defensive measures may lead to a security dilemma that precipitates an arms race and ultimately undermines alliance unity.

ESCALATION RISKS IN THE BALTICS

The challenge Russia poses, combined with NATO’s responses to date, creates a series of potential escalation pathways, which need allies’ urgent attention.

The Pitfalls of NATO’s Trip Wire Approach

The alliance’s need to reinforce troops in a crisis and the positioning of some of its forces in the region could spark inadvertent or deliberate escalation.

• Were Russia to threaten military escalation in a crisis, NATO would feel significant pressure to reinforce forward-deployed troops as a defensive precaution. However, if NATO failed to clearly and persuasively communicate to Russia its defensive intent, Moscow might misread the deployment as the opening of a NATO offensive, perhaps responding by escalating to (what the Kremlin would see as) the preventive use of military force.

• As soon as NATO was to send in reinforcements (or even, perhaps, when Moscow was to judge the alliance was about to do so), Russia might try to use its anti-access/area denial (A2/AD) capabilities around the Baltic Sea to cut off sea and air routes. NATO might, therefore, believe it has little choice other than to attack Russian A2/AD capabilities early in a conflict, effectively escalating conflict into Russian territory.

• Even more concerning, were Russia to use force against the alliance by taking a small portion of land in, for instance, eastern Latvia, EFP forces, which are based far from the Russian border, might arrive too late to engage in combat (especially given that NATO’s decisionmaking process could be quite slow). Consequently, Russia might hope to get away with a military fait accompli.

• NATO’s combined conventional military power and any subsequent efforts to retake the Baltics through massive force deployments, once initiated, would put the onus on Moscow. Out of fear of losing a conventional conflict with NATO, Russia might escalate further, perhaps even to nuclear use.

Ambiguous Nuclear Doctrines Ambiguities in NATO’s and Russia’s nuclear policies create the potential for deliberate escalation. • NATO allies have disagreed about the politics of nuclear sharing, the idea of having nonnuclear NATO members take part in nuclear planning and some members providing national aircraft to deliver U.S. nuclear weapons in the event of their use. In addition, allies disagree about the appropriate readiness levels for those dual-capable aircraft in Europe and about whether NATO exercises should involve nuclear elements. This somewhat ambiguous stance toward nuclear deterrence might lead Russia (perhaps wrongly) to doubt NATO’s resolve in a crisis, increasing the risk of escalation. • Conversely, NATO might not view Russian nuclear threats as credible, especially early in a crisis when they might appear to be disproportionate. In this case, NATO misreading Russian resolve might cause escalation.

Nonkinetic Operations

Moscow’s efforts to influence Russian minorities in the three Baltic states could lead to a crisis in which neither NATO nor Russia would be able to manage subsequent escalation.

• For many years, Russia has staged a subversive disinformation campaign in the Baltics, aimed at influencing Russian minorities. If protests by these minorities were to occur—whether deliberately fomented by Moscow or not—NATO and Russia might find it difficult to deescalate the initial stages of a crisis and instead might get drawn into an action-reaction cycle, even though neither side would want it to spiral out of control.

• In such a scenario, given the possibility of Russia’s building up forces in proximity to Baltic borders, it is not clear what role NATO forces, particularly the EFP, could or should play. NATO would have to balance the risks of escalating early against waiting too long, and the alliance might find it challenging to identify when a crisis would warrant a military response and what that response might be.

Dangerous Military Incidents

Russia’s continued military brinkmanship (by its aircraft, in particular) coupled with inadequate crisis communication tools could trigger accidental escalation.

• An accidental military incident—such as a Russian fighter jet accidentally crashing into a U.S. destroyer in the Baltic Sea—could escalate rapidly. European NATO members might prefer to deal with such an incident as an alliance, whereas Washington would probably prefer not to. As a result, NATO might not only be weakened by infighting but the U.S.-Russian action-reaction cycle might unfold more rapidly than multilateral efforts to clarify what occurred and to deescalate the crisis. In addition, existing crisis communication channels with Russia might not be used to prevent escalation in the wake of such an accident.

#### Goes nuclear. Russia’s escalate-to-deescalate doctrine.

NSNWs = non-strategic nuclear weapons

TNWs = tactical nuclear weapons

Brookes 22 [Dr. Peter Brookes, Heritage Foundation senior fellow and a former U.S. Deputy Assistant Secretary of Defense; 3-5-2022; "Russia’s Small Nukes are a Big Problem for European Security"; Monitor Strategic; https://ispaim.mapn.ro/webroot/fileslib/upload/files/Monitor%20Strategic/ms122022.pdf#page=47; KL]

With Russia’s ongoing war in Ukraine, now is a good time to take note of a little-spoken-of, but glaring, imbalance between America’s and Russia’s nuclear arsenals—and how it could affect stability in Europe and the interests of the United States and those of its European allies and partners.

If asked, many Americans and Europeans probably believe that the United States and Russia are pretty evenly matched in terms of the number of nuclear weapons both sides have in their arsenals. While their beliefs are entirely understandable, they are not completely correct

Under the 2010 bilateral New Strategic Arms Reduction Treaty—also known as New START—the United States and Russia have a similar number of deployed strategic (i.e., high-yield and long-range) nuclear weapons: 1,550 deployed nuclear warheads each.1 But not all of Washington’s or Moscow’s nuclear weapons are covered by New START.

Indeed, Russia has nearly a 10:1 advantage over the United States and NATO in non-strategic (i.e., low-yield and short-range) nuclear weapons (NSNWs).2

Assessments based on open sources estimate that Russia has about 2,000 NSNWs. It is similarly assessed that the United States and NATO have about 200 NSNWs in their arsenal.3 It is postulated that half of those U.S.-NATO weapons are located in the United States and half are based in Europe as part of NATO’s nuclear forces.4

While capable of significant destruction, these tactical nuclear weapons are lower in yield – or explosive power – and are meant for use on the battlefield against military installations or troop and equipment concentrations as opposed for use against counterforce or countervalue targets such as ICBM missile fields, command and control nodes, and or population centers (e.g., cities).

It is believed that Russia can deploy these weapons on multiple tactical systems including dual-capable short-range or theater ballistic missiles, torpedoes, and anti-ship missiles.5 Indeed, it is expected that Russia’s new hypersonic weapons may be dual-capable (i.e., conventional or nuclear armed) as well.6

Major nuclear weapons states, including Russia, have said that a nuclear war could never be won and therefore should never be fought. However, there are deep concerns among policy makers and security analysts outside Russia about whether Moscow fully embraces that idea or if it is just convenient diplomatic rhetoric.

Also of increasing concern is a Russian military doctrine associated with battlefield nuclear weapons known as “escalate to deescalate.” This topic is of particularly interest right now with the war in Ukraine ongoing since late February 2022. According to the 2018 U.S. Nuclear Posture Review (NPR):

“Russia considers the United States and the North Atlantic Treaty Organization (NATO) to be the principal threats to its contemporary geopolitical ambitions. Russian strategy and doctrine emphasize the potential coercive and military uses of nuclear weapons. It mistakenly assesses that the threat of nuclear escalation or actual first use of nuclear weapons would serve to “de-escalate” a conflict on terms favorable to Russia. These mistaken perceptions increase the prospect for dangerous miscalculation and escalation.”7

The NPR further asserts that:

“Moscow threatens and exercises limited nuclear first use, suggesting a mistaken expectation that coercive nuclear threats or limited first use could paralyze the United States and NATO and thereby end a conflict on terms favorable to Russia. Some in the United States refer to this as Russia’s “escalate to de-escalate” doctrine. “Deescalation” in this sense follows from Moscow’s mistaken assumption of Western capitulation on terms favorable to Moscow.”8

Though the Russians seemingly refute the existence of this doctrine by its American name at least, some sources assert that the policy may actually have been developed in the late 1990s, when now-Russian President Vladimir Putin was chairman of the Russian National Security Council under President Boris Yeltsin.9

The idea behind escalate to deescalate is that Russia might employ one tactical nuclear weapon (or more) during a conventional conflict with NATO forces for the purposes of preventing a defeat, consolidating territorial gains, or even freezing a conflict in place without the prospect of further fighting.

Indeed, because of the large, nearly 10:1 disparity between the number of Russian and U.S. tactical nuclear weapons, Moscow may think a nuclear response from NATO is not a credible threat due to Russia’s asymmetric advantage. Other factors may also play a role in Russian calculations, including a perception that NATO’s large membership would have difficulty finding a political-military consensus on an appropriate response, including a nuclear option.

An example of the potential use of this Russian nuclear doctrine in a hypothetical scenario might be helpful here:

Moscow attacks one—or all—of the Baltic States with its conventional forces to establish control over some, or all, of these nations’ territory, returning them to Russia’s control as they were in the Soviet era. Invoking Article V, NATO responds with conventional forces to protect and restore the sovereignty of these three allied states.

Concerned about the inferiority of its conventional forces in this fight against the allied powers, Moscow then contemplates exploding a low-yield tactical nuclear weapon somewhere in theater as a warning of Russia’s potential escalation from the conventional to the nuclear domain of warfare, including the potential future use of high-yield, strategic nuclear weapons.

In Moscow’s eyes, perhaps NATO will become concerned about the possible escalation of the fighting from the conventional to the nuclear—especially Russia’s potential use of more powerful nuclear weapons against European and American cities. In response, NATO may consider pausing its counteroffensive against Russian forces in the Baltics.

Indeed, Moscow may misperceive that if NATO does not have sufficient tactical nuclear weapon capabilities to respond in kind, it would be inclined to seek de-escalation rather than launch a strategic nuclear weapon at Russia and risk moving further up the escalation ladder—a response that could lead to all-out nuclear war.

Using its tactical nuclear weapon advantage over NATO and having strategic nuclear parity with Washington, Moscow could threaten additional low-yield nuclear strikes unless fighting ends on Russia’s terms. Ideally for Moscow, NATO might decide that there is no good option available to respond and chooses to cease hostilities, locking in Moscow’s ill-gotten gains in the Baltics.

With these political-military calculations in mind, Russia takes a chance on the expected NATO response and explodes a 10-kiloton tactical nuclear weapon near or in the European theater. As a result, nuclear deterrence fails for the first time in history not due to the use of strategic nuclear weapons that so many people are aware of, but the imbalance of battlefield nuclear weapons between NATO and Russia.

## Cyber---AT: Squo Deployments

#### Deployments are symbolic and aren’t going to the Baltics.

Birnbaum and Rauhala 22 [Michael Birnbaum, reporter covering climate and security; Emily Rauhala, Brussels bureau chief; 6-29-2022; "Those 300,000 high-readiness NATO troops? ‘Concept,’ not reality."; Washington Post; https://www.washingtonpost.com/world/2022/06/29/those-300000-high-readiness-nato-troops-concept-not-reality/; KL]

On Monday, NATO Secretary General Jens Stoltenberg announced plans to put 300,000 troops at high readiness as part of the “biggest overhaul of our collective defense and deterrence since the Cold War.”

By Wednesday, as NATO leaders gathered at a summit in Madrid, the vast new mobilization appeared to be more fearsome on paper than in reality, more of an aspiration than a dramatic new commitment to defend Europe.

Stoltenberg’s announcement caught the top defense officials of many NATO members off guard, leading them to question which of their forces, if any, were being included in the 300,000 figure.

“Maybe it’s number magic?” said one senior European defense official, who, like others, spoke on the condition of anonymity to talk frankly about the confusion.

Several senior European security policymakers said they were taken by surprise, with no advance notice of the plan to expand NATO’s quick-response force from its current size of 40,000 in light of the Ukraine war and Russia’s ongoing military threats to NATO territory.

A senior defense official from a different alliance country said its leaders had not been consulted about the figure ahead of time. The official wondered which of his nation’s troops were being counted toward the force — and whether it included personnel from a volunteer national guard who have civilian day jobs.

Asked at a news conference on Wednesday about the mystery of the missing troops, Stoltenberg said the “majority” will be based inside their home countries and will build on existing personnel — code, in some ways, for simply reclassifying troops that currently exist and making them more available for fast deployment under NATO command in the event of a security crisis.

“Of course it requires, as always when you do something in NATO, that allies contribute the forces they have promised to contribute,” he said, not directly addressing why some countries apparently have not yet been asked about stepping up.

Stoltenberg said he hopes to have the expanded rapid force available sometime next year.

A NATO official, speaking on the condition of anonymity per the alliance’s ground rules, said that country-specific numbers still needed pinning down. Even the 300,000 total is theoretical for the moment: “The concept has not been fully worked up yet,” the official said. “We will have to do more to build up the model before we can work out what national commitments can be.”

# Modeling Advantage Cards

### Warming

#### NATO involvement is key to overcome dependence

ÇAlışMa Grupları, Diplomasigeneluluslararası, which is a very important job in another language İLişKiler· 4-28- 2022·, "The Energy Security of the Baltic States and the Tensions with Russia," TESAD, https://www.tesadernegi.org/the-energy-security-of-the-baltic-states-and-the-tensions-with-russia.html//DG

The last term applies to the interconnection between the Baltic States and Russia as the Baltics are considered vulnerable and a trade war could drag them down in a crisis[45]. Since the Baltic market is not economically important to Russia, the interdependence is considered asymmetrical. Russian exports for the year 2020 to Latvia were 2.23B, Estonia $2.59B, and Lithuania $2.39B[46]. Nevertheless, from the opening of the Balticconnector and other interconnections belonging to the European network the region plays an important role in gas and petroleum transit, ensuring the uninterrupted flow of energy to further European destinations. Consequently, the Kremlin started to look around for solutions and has developed a strategy comprising the construction of alternative routes, namely the Nord Stream 1 and 2, the Turkish Stream and the Power of Siberia pipelines.

However, the complex situation must be framed inside a broader strategic vision according to Keohane’s and Nye’s interdependence theory. Russian weight in the Baltic energy security undergoes military security conditions. The Baltic States are part of the eastern flank of NATO, therefore their integration into the Russian energy infrastructure is meant to balance the presence of the Western military alliance in the region[47]. Moreover, the Baltics register a high presence of Russian immigrants in their populations, thus energy is used as a weapon to prevent any kind of discrimination.

The request of the Estonian Defence minister for a strengthening of NATO’s presence in the Baltics following the outbreak of the Russian-Ukrainian conflict in 2022 reflects well the interdependence hypothesis. Estonia, likewise, its neighbours, fears the extension of the conflict to the area and the possibility of retaliation in the energy sector, as the country has engaged itself actively in the reception of war refugees from Ukraine[48]. According to the Bank of Estonia, the outbreak of war has influenced markets, prices of natural gas and electricity are increasing, and households’ consumption is expected to reduce in the short term. Therefore, the Estonian government decided to place natural gas and heating under a price ceiling until spring 2022[49]. Lithuania on its side is bringing forward the GIPL project with Poland and is looking forward to opening the pipeline ahead of schedule, on May 1st. The three countries foresee closer regional and European cooperation to reduce their dependence.

In the past, Russia could benefit from the European uncertainty due to the different levels of European involvement in the matter and the controversy in the support of stronger sanctions. But a comprehensive energy network has been developed in the past twenty years and now the European Union presents itself as a single and active actor in the international environment, that stands for the democratic values and is ready to defend itself against external claims of special interest zones in the former Soviet space[50]. For the Baltic States, this means knowing that they can fully lean on Western support in asserting their own sovereignty.

Therefore, to reinforce its self-determination, the European Union launched the REPower plan in March 2022, aiming at phasing out the fossil fuels import dependence from Russia. The strategy requires the almost complete filling up of the capacity gas stock storage before winter, the replacement of gas in heating and power generation and more renewables investments[51].

#### Baltic renewables k2 european green energy transition

Lukas Trakimavičius, 3-19-2021, Trakimavičius works at the Research and Lessons Learned Division of the NATO Energy Security Centre of Excellence "The untapped green energy potential of the Baltic States," euractiv, https://www.euractiv.com/section/energy/opinion/the-untapped-green-energy-potential-of-the-baltic-states//DG

As the global energy transition gathers speed, the Baltics may not seem like its obvious frontrunners. Despite making great strides in making their energy systems cleaner, fossil fuels still remain a staple of their energy diet. However, growing evidence suggests that the Baltics have a massive offshore wind energy potential, which could have a game-changing effect for the entire region. Chances are, wind turbines could not only propel the Baltics to the forefront of the energy transition, but also to the ranks of clean energy exporters. As things stand, few would argue that the Baltics are on the cutting edge of the clean energy transition. Like most of their European peers, they get the bulk of their energy from fossil fuels such as oil and natural gas. These are either imported from far abroad or, as is the case with Estonian oil shale, mined from deep underground. Meanwhile, renewables such as onshore wind, solar or hydropower still account for a tiny fraction of their overall energy needs. In 2019, these energy sources met some 2.6 percent of [Lithuania](https://www.iea.org/countries/lithuania)’s, 4.6 percent of [Latvia](https://www.iea.org/countries/latvia)’s and 1.3 percent of [Estonia](https://www.iea.org/countries/estonia)’s total primary energy demand. Granted, the overall share of renewables is vastly greater once biomass is added into the mix. Yet, some scientists [argue](https://ec.europa.eu/jrc/en/publication/eur-scientific-and-technical-research-reports/use-woody-biomass-energy-production-eu) that fuels such as firewood or wood pellets may not be the most environmentally sustainable sources of energy. However, what the Baltics lack in fossil fuels, they make up for with an abundance of wind in the Baltic Sea, which can be harnessed and converted into electricity. Though currently none of the Baltics have any windmills in the open seas, all three have major offshore wind plans for the future. Lithuania, for example, intends to [have](https://enmin.lrv.lt/en/news/offshore-wind-another-direction-of-renewable-energy-to-strengthen-local-power-generation-in-lithuania) at least 700 megawatt (MW) of offshore wind farms in operation by 2030. Latvia and Estonia are also eying to co-develop a [joint](https://www.windpowermonthly.com/article/1690879/estonia-latvia-sign-pact-1gw-offshore-wind-farm) 1,000 MW wind farm in the Gulf of Riga. On top of that, Estonia [wants](https://news.err.ee/1149566/dutch-company-van-oord-buys-stake-in-saare-wind-energy) to have a 1,000 MW offshore wind park near the island of Saarema by 2028, in addition to a slew of other projects that are under [consideration](https://www.windpowermonthly.com/article/1690879/estonia-latvia-sign-pact-1gw-offshore-wind-farm).All of this sounds great, but it could just be the beginning. According to a recent WindEurope [study](https://windeurope.org/wp-content/uploads/files/about-wind/reports/WindEurope-Our-Energy-Our-Future.pdf), the Baltic Sea could be the next big thing for Europe’s energy transition. It is estimated that Lithuania [could](https://windeurope.org/wp-content/uploads/files/about-wind/reports/WindEurope-Our-Energy-Our-Future.pdf) have up to 3,600 MW, Latvia up to 2,900 MW and Estonia up to 1,500 MW of offshore windfarms by 2050. If this generation capacity could be met, the study claims that the Baltics could potentially [export](https://windeurope.org/wp-content/uploads/files/about-wind/reports/WindEurope-Our-Energy-Our-Future.pdf) around half of their offshore wind electricity to neighboring states. Obviously, it is difficult to say with certainty just how much electricity would the Baltics be able to export and others would like to import. After all, to get to a zero-carbon future, the Baltics and their neighbors will have to [undergo](https://www.weforum.org/agenda/2020/04/can-electricity-decarbonize-the-energy-sector/) tremendous changes by 2050. Not only will they have to make energy use more efficient, but they will also have to decarbonize and electrify large portions of their economies. Still, if the Baltics would harness their full offshore wind potential and would continue to develop other renewable sources of energy, there are few doubts that a good chunk of their electricity might still be available for export. To get more bang for the buck, the Baltics could also take some of this newfound electricity and transform it into green hydrogen using a process known as electrolysis. Green hydrogen could be used for manufacturing, transport, heating or [converted](https://www.scientificamerican.com/article/solar-and-wind-power-could-ignite-a-hydrogen-energy-comeback/) back into electricity to back up the grid. Or it could simply be exported to neighbouring states. This step would prevent excess electricity from being wasted and also help decarbonise those sectors of the economy where electrification is difficult.

#### European transition checks warming---else, all other renewables fail

EEA, European Environment Agency 8-1-2017, "Energy and climate change," European Environment Agency, https://www.eea.europa.eu/signals/signals-2017/articles/energy-and-climate-change//DG

The global climate is changing and that is posing increasingly severe risks for ecosystems, human health and the economy. The EEA’s recent assessment ‘[Climate change, impacts and vulnerability in Europe 2016](http://www.eea.europa.eu/publications/climate-change-impacts-and-vulnerability-2016)’ shows that Europe’s regions, too, are already facing impacts of a changing climate, including rising sea levels, more extreme weather, flooding, droughts and storms.

These changes are happening because large amounts of greenhouse gases are released into the atmosphere as a result of many human activities worldwide, including, most importantly, burning fossil fuels for electricity generation, heating and transport. Combustion of fossil fuels also releases air pollutants that harm the environment and human health.

Globally, the use of energy represents by far the largest source of greenhouse gas emissions from human activities. About [two thirds of global greenhouse gas emissions](http://www.iea.org/publications/freepublications/publication/CO2EmissionsfromFuelCombustion_Highlights_2016.pdf) are linked to burning fossil fuels for energy to be used for heating, electricity, transport and industry. In Europe, too, the energy processes are the largest emitter of greenhouse gases, being responsible for 78 % of total EU emissions in 2015.

Our use and production of energy have a massive impact on the climate and the converse is also increasingly true. Climate change can alter our energy generation potential and energy needs. For example, changes to the water cycle have an impact on hydropower, and warmer temperatures increase the energy demand for cooling in the summer, while decreasing the demand for heating in the winter.

Global efforts so far to mitigate climate change culminated in the [Paris Agreement](http://unfccc.int/paris_agreement/items/9485.php) in 2015. Through the agreement, 195 countries adopted the first-ever universal and legally binding, global climate deal. The target of the agreement — limiting the global average temperature rise to well below 2 °C, while aiming to limit the increase to 1.5 °C — is ambitious and cannot be achieved without a major overhaul of global energy production and consumption.

To support the global climate agenda, the EU has adopted binding climate and energy targets for 2020 and proposed targets for 2030 as part of its overall efforts to move to a low-carbon economy and to cut greenhouse gas emissions by 80-95 % by 2050. The first set of climate and energy targets for 2020 includes a 20 % cut in greenhouse gas emissions (compared with 1990 levels), 20 % of energy consumption coming from renewables and a 20 % improvement in energy efficiency. Based on the current proposals in discussion in EU institutions, the next milestone of 2030 pushes these targets to a 40 % cut in emissions, 27 % of energy coming from renewable sources and a 27 % improvement in energy efficiency (or 30 %, as recently proposed by the European Commission) compared with baseline.

### Taiwan

#### Taiwan models. They face similar risks.

Sprūds 22 [Andris Sprūds, Director of the Latvian Institute of International Affairs; Una Aleksandra Bērziņa Čerenkova, Head of the Asia program at the Latvian Institute of International Affairs; Sintija Broka, Researcher at the Latvian Institute of International Affairs; 2022; "Note From the Editors"; *Hybrid Threats in Baltics and Taiwan: Commonalities, Risks and Lessons for Small Democracies*; https://www.baltdefcol.org/files/files/publications/Hybrid%20Threats\_LIIA.pdf#page=38; KL]

The year 2022 brings the globe into a period of what could be described with the oxymoron “stable uncertainty”. Societies around the world are adapting to living their lives and making decisions against the backdrop of the everdeveloping COVID-19 pandemic, and the constant lingering feeling of not knowing what tomorrow holds is neither new nor shocking anymore. The conundrum of “stable uncertainty”, however, exacerbates and facilitates other diverse challenges, to which we commonly refer as hybrid threats.

The Baltics as well as Taiwan have been facing uncertainties caused by risks to political legitimacy, societal resilience, critical infrastructure, energy security, and cyber security long before the world went into lockdown – and long enough to have developed a certain resilience. It is a resilience that stems from unique, but translatable experiences of small, yet resourceful democracies. The goal of the Latvian Institute of International Affairs publication “Commonalities, risks, and lessons for small democracies: hybrid threats in Baltics and Taiwan” is to take stock of these experiences and their regional manifestations, to draw parallels between the threats that caused them, to map the risks we’re still facing, and to present wider lessons based both on the successes and tribulations of the Baltic states and Taiwan. The volume is designed to provide an overview of how the Baltic states of Lithuania, Latvia and Estonia on one side and Taiwan on the other face, combat and conceptualize hybrid threats.

#### 5G cyber is the new battlefield, mutual cooperation between US-NATO with the Baltics key to combat China and Russia

Wierenga 22 (Louis Wierenga Junior Research Fellow, Johan Skytte Institute of Political Studies, University of Tartu | Lecturer in International Relations, Department of Political and Strategic Studies, Baltic Defence College. “Cybersecurity and Hybrid Threats in the Digital Baltic states: A state of the art”, https://www.baltdefcol.org/files/files/publications/Hybrid%20Threats\_LIIA.pdf)LR

In light of power competition vis-à-vis cooperation with the US, NATO, and the EU, and small states standing up to larger powers with nefarious intentions, the drawback is that no entity is capable of defeating all cyberattacks; rather, in order to succeed in cyberspace, the key is learning how to adequately *cope.*24 When it comes to information warfare, and one of the reasons for which it is so dangerous, is that the antagonist need not win – they succeed if they are able to successfully cloud the issue.25 It is no secret that **Russia has waged** **numerous information warfare campaigns in the Baltics** and show no sign of giving up. Recommendations and policy developments Keep on the cusp of cyber hygiene and widely promote amongst citizens: General H.R. McMaster notes the importance of American efforts to conduct reconnaissance in cyberspace and preempt attacks.26 Strive to continuously be one step ahead of hackers. Although this is a daunting, if not (nearly) impossible task, it is one which would involve both governments and the general public. One aspect which has greatly contributed to the success of Estonia in becoming a world leader in cyber defence is investing in people.27 Promoting cyber hygiene is one aspect at which Estonia excels. Raising further awareness about media literacy to combat disinformation and misinformation also helps to win the battle against information warfare. McMaster also advocates for the US to learn from countries which were on the receiving end of Russian aggression.28 As one of the strengths which Estonia possesses is its investment in people, Estonia is a success story in cyber and IT education and training, ranging from kindergarteners to the elderly.29 In an increasingly multipolar world order**, the rise of China presents a serious security challenge** to Europe and the Transatlantic alliance and can be seen on a number of fronts. One of the most pressing, especially when it comes to cybersecurity, is 5G. If seen through the lens of ‘the West’, then a united front should consist of the US and NATO, plus PfP countries, along with the EU in cyber policy. When it comes to 5G, this is especially important. The Baltic states have taken strides to become leaders in 5G policy and can use this opportunity to take a leading role in a Western front in the battlegrounds for 5G policy. Keeping focus on both China and Russia as threats to the security of NATO and the EU: For valid reasons – both historical and contemporary – the Russian Federation is identified as the primary security threat to the 3 Baltic states. The most contemporary events in the neighborhood do not indicate any change in the consistency or persistence of the threat, nor its digital nature. Cyber and hybrid threats directed towards the Baltic states from the Russian Federation will not cease and military, government, and civilian entities need to continue with vigilance, adapt to the rapidly changing nature of cybersecurity and cyberwar, as well as anticipate future changes, staying ahead of the curve. However, despite the very valid concerns over Russian cyber activity, the Baltic states should not neglect such concerns as they relate to China. Indeed, as aforementioned, the Baltic states, especially Lithuania, have taken a firm stance towards China, in cyberspace and beyond, and should continue to use their growing digital prowess to expand their influence in the EU and NATO. Lithuania, under the leadership of Foreign Minister Gabrielius 63 Landsbergis, has increasingly stood up to China.30 Minister Landsbergis’s stance towards China led to him being named as one of Politico’s ‘most influential people in Europe’ – and the only one to make the list from any of the Baltic states.31 Latvia has called upon China to respect the rules of international cyberspace.32 It should be noted that this is certainly not the first time that leaders from the Baltic states have appeared on similar lists, granting small states representation on lists where the usual larger powers within Europe enjoy substantial representation. Such leadership should be emulated, and the digital advances made by the Baltic states provides an ideal way to achieve this, as many countries look to the Baltics as digital leaders. Demonstrating leadership to allies: If ever there was a time, as well as a concrete area for the Baltic states to showcase their strengths as small states, demonstrating leadership in the cyber and tech fields presents the perfect opportunity. Estonia has been the Baltic champion for cybersecurity and e-governance. Lithuania, and to a lesser extent Latvia have shown signs of catching up. Much like offline matters, the three Baltic states use opportunities to meet with US and EU leaders to highlight the dire security situation which the Transatlantic alliance faces from a resurgent Russia – they know from experience and contemporary matters. As the security of cyberspace is one of the acute questions of global politics this century33, cybersecurity and matters of digital warfare will be issues which merit pressing resolve, which is constantly changing. Being on the cutting edge will require countries to remain that way. While member of the United Nations Security Council for the first time, Estonia made cybersecurity a priority, along with the overall security of the region.34 As well, when a member of the UN Security Council, Estonia made it a point to align with the US and the UK to call Russia out over a cyberattack directed at Georgia.35 Latvia and Lithuania have also been active on such fronts. In 2021, Latvia signed an agreement with Poland which establishes a framework for cooperation between Latvia’s Military Information Technology Security 64 Incident Team (MilCERT) and Poland’s National Cyber Security Center.36 Latvia is also taking the opportunity to reach out to the United States to discuss cybersecurity in the region.37 Lithuania has, as aforementioned, developed their own cyber center the RCDC, which is a bilateral LithuanianUS initiative.38 Conclusion To conclude, the domain of cyberspace will be an arena for battle for the foreseeable future. All countries, governments, militaries will be faced with such threats, and the likelihood of businesses and private individuals being faced with such threats is high. The Baltic states are no strangers to such threats and have been leaders in facing up to them. Given the nature of threats faced and the manner in which the Baltics have faced up to them, it is safe to say that the Baltic states will continue to rise up to the challenges and keep up with the rapidly changing nature of cyber threats. However, the last point is the most persisting challenge any entity faces in cyberspace – the need to not only consistently keep up but remain steps ahead of adversaries. The bi- and multilateral agreements made as well as the leadership demonstrated, and the digital awareness can go a long way to not only meet contemporary and future challenges but serve as examples and demonstrate leadership. Cyber and hybrid threats are ominous, but on a positive note, the Baltic states have achieved many remarkable accomplishments in this field.

#### Strengthening Baltic cyber security spurs Taiwan-Lithuania cooperation

Cole 21 (J. Michael Cole, Senior Advisor, Countering Foreign Authoritarian Influence (CFAI) at the International Republican Institute (IRI); Global Taiwan Institute, Macdonald-Laurier Institute, Prospect Foundation. Senior Non-Resident Fellow @ Global Taiwan Institute, Masters in War Studies @ Royal Military College of Canada, International Diploma in Humanitarian Assistance @ Fordham University. “The Lithuanian model for expanding Taiwan’s ties with Baltic States”, https://www.caribbeannewsglobal.com/the-lithuanian-model-for-expanding-taiwans-ties-with-baltic-states/)LR

The establishment of a representative office in Lithuania constitutes a victory for Taiwan in its efforts to counter both international isolation and the Chinese narrative of Taiwan’s supposedly inevitable international isolation. By focusing on a part of the world that has not traditionally been an area for Taiwanese presence and engagement, Taipei has also demonstrated the virtues of an asymmetrical approach to combating China on the world stage. This development also exposes the fact that Beijing is willing to break its own rules on “One China,” in that it is now willing to punish states even when they continue to abide by their “One-China Policy” by not establishing official ties with Taiwan. Although the object of Beijing’s ire is ostensibly related to the nomenclature used for Taiwan’s office in Vilnius (which uses the word “Taiwan”), at a deeper level, the source of its anger is the gains that Taiwan has made in Europe, an area where China had hoped to increase its influence. Lithuania has taken some risks in placing its bets on Taiwan, and besides the retaliation it is currently facing, the move may also have cost it future economic opportunities. Consequently, it will be crucial for Taiwan to demonstrate that Vilnius’ risk-taking was not in vain. Already, a large Taiwanese trade and investment delegation has visited the country, with a total of 240 online and offline trade talks involving more than 150 Lithuanian firms and various Taiwanese ones. Taiwan must build on the complementarity of the two economies to replicate its successes in countries like the Czech Republic, where despite much Chinese propaganda, Taiwan has been a much more substantial investor and job creator. Lithuania has a hard-working, highly educated and productive workforce in the manufacturing sector, with strengths in areas such as the laser industry—which has also become a target for Chinese retaliation, with China deciding to halt cooperation between its laser industry bodies and Lithuania. Trade forms the basis of bilateral relations and must be mutually beneficial. Lithuania has made it clear that it expects to reap the benefits of engagement with Taiwan, a country with an economy approximately 11 times larger than its own, as well as a highly advanced tech sector. Lithuania therefore represents a golden opportunity for Taiwan to showcase the advantages of engagement and to demonstrate that small and medium states not only can afford to defy China but can actually benefit materially from doing so. Conversely, failure to build upon and to sustain this momentum could dissuade prospective partners from going down that path. Thus, Taipei must demonstrate a commitment to building prosperous and mutually beneficial ties with its new Baltic ally, and the tangible results must materialize as expeditiously as possible. The potential for engagement between Taiwan and the Baltics goes well beyond trade and investment, however. Lithuania, Latvia, and Estonia all have traditions of resistance to external aggression and, by virtue of their proximity to Russia, have developed their own strategies to counter the security threat posed by their much more powerful – and like China, expansionist neighbor. Taiwan and the Baltic states, therefore, have much to learn from each other, in areas ranging from cyber and hybrid warfare to the implementation of an asymmetrical defense posture. While Russia poses the more immediate threat to the Baltic region underscored by apprehensions across the region that Moscow could launch an invasion of Ukraine as early as next January – it is also clear that China has become a more active player in the region, with all the risks of espionage, cyberattacks, co-optation, and hybrid threats that this new presence entails. Countries like Lithuania that have already defied Beijing are now bracing for the very real possibility of cyberattacks against their institutions, and this is an area where Taiwan’s expertise in addressing such threats can come in handy. **Appropriate intelligence-sharing mechanisms** must therefore be established to facilitate communication, threat mitigation, and response; these are areas where, again, Baltic states can make real gains from a deeper relationship with Taiwan, whose capabilities in the cyber sector are larger by orders of magnitude. The fledgling relationship with this part of Europe also creates opportunities for Taiwan’s indigenous defense industry, particularly in the unmanned vehicle sector: for example, Taiwan donated 10 police drones to Lithuania in October to assist the country as it deals with an influx of refugees from Belarus. For its part, Taiwan has much to learn from the Baltic states in non-traditional military areas, particularly in areas of state resilience and the concept of total defense. For example, as it explores ways by which to increase its deterrence against a Chinese attack, the Taiwanese military could learn important lessons from the Lithuanian Lietuvos Šaulių Sąjunga (“Riflemen’s Union”), the Estonian Defense League, and the National Guard, initiatives that blend traditional military forces with a militia and civilian component. Among other things, Taiwan could learn from those countries’ experiences in providing training to these additional layers of defense, as well as how and where to safely store weapons so that they can be quickly accessed by paramilitary forces in times of national emergency. No doubt Taiwan could learn a thing or two about forming and training a proper Reserve Force. Taiwan and the Baltics can also identify areas for the joint training of special forces and other units charged with waging asymmetrical war against a much more powerful and better-equipped opponent. Latvia and Lithuania, in particular, have clearly signaled their willingness to engage Taiwan more closely on such matters. For this to happen, the Taiwanese government will have to be willing to go beyond its traditional areas of engagement on security issues, and civilian authorities will have to contend with a culture of historical resistance within the ministry of national defense to the idea of giving the population a role in national security (especially one that involves arming them). But as with trade, Taipei will need to overcome those difficulties and, as rapidly as possible, demonstrate to its potential partners that it is ready to engage them in a way that is mutually beneficial. As the experience with Lithuania shows, an unprecedented window of opportunity has been created for Taiwan in the Baltics -one that will not remain open indefinitely. While we cannot expect results overnight, especially on security matters, Taipei cannot afford to drag its feet – and must therefore be proactive in its efforts to turn this potential into a source of real benefits for all the countries involved. It has natural and willing partners in the Baltics; Taipei, too, must demonstrate that it means what it says. If it does well in that area, there is a high likelihood that countries elsewhere will take notice. Failure to seize this moment, however, could have long-term detrimental effects on Taiwan’s appeal, and thereby strengthen China’s ability to deter engagement with Taiwan. The ball, therefore, is very much in Taipei’s court. The main point: A window of opportunity has opened for Taiwan to deepen its engagement with the Baltic states, a grouping of small nations that also faces an existential threat from a powerful authoritarian neighbor. In areas ranging from trade to non-traditional defense, these states are natural allies for Taiwan, and provide a chance for Taipei to showcase the real benefits of closer ties despite threatened retaliation by Beijing.

#### \*\*\*Chinese cyberattacks destabilize Taiwan

* Cyber - -> invasion and PRC can destabilize/counter US forces

Sacks 22 (David, research fellow at the Council on Foreign Relations, where his work focuses on U.S.-China relations, U.S.-Taiwan relations, Chinese foreign policy, cross-Strait relations, and the political thought of Hans Morgenthau. “Enhancing U.S.-Japan Coordination for a Taiwan Conflict”, https://cdn.cfr.org/sites/default/files/report\_pdf/Enhancing%20U.S.-Japan%20Coordination%20for%20a%20Taiwan%20Conflict\_DP\_1.pdf)LR

Adding to the worry, over the past five years China has steadily increased its pressure on Taiwan, reducing the number of mainland tourists who can visit the island, stripping away its few remaining diplomatic partners, placing an embargo on certain Taiwanese exports, ramping up military activities in its vicinity, conducting cyber-attacks, and interfering in Taiwan s democratic process. While Xi continues to publicly stress his commitment to peaceful reunification” with Taiwan and has not introduced an explicit timeline for achieving this objective, he has also said that the Taiwan issue cannot be passed on from generation to generation.”2 He has set 2049 as the date by which China must achieve the great rejuvenation of the Chinese nation,” and achieving reunification” with Taiwan is a core condition for that project.3 Still, it remains unlikely that Xi has already decided to use force against Taiwan, which provides an opening for the United States to adjust its policies and work with its allies to help prevent such an outcome. Although there is debate over whether China will resort to force, China is clearly developing capabilities needed to invade and occupy Taiwan. Preparing for a conflict over Taiwan has driven China s military modernization campaign for the past two and a half decades. China has invested significant resources in developing the tools to defeat Taiwan and prevent the United States from coming to its aid, principally an arsenal of accurate ballistic missiles, the world’s largest navy, hundreds of modern fighter aircraft and bombers, and advanced cyber and counterspace assets The recommendations proposed, while ambitious, are feasible in the current political climate in both Washington and Tokyo, and, with sustained focus in both capitals, can be implemented in the next five years. While China has a number of options it could take to put pressure on Taiwan—seizing an offshore island, initiating massive cyberattacks, firing hundreds of ballistic missiles to take out critical infrastructure, and conducting a quarantine of the island—this paper focuses squarely on how to deter and respond to an invasion of Taiwan. It does so in the belief that Japan s appetite for assisting the United States in countering Chinese aggression against Taiwan short of a full war is politically challenging and likely limited. China is not relying on its inherent advantages, however, and has instead spent the last two and a half decades developing capabilities designed to neutralize U.S. power in the Taiwan Strait. Its military budget has grown from $14.3 billion in 1996 to $252.3 billion in 2020, a nearly eighteenfold increase (see figure 2).7 Preparing for a conflict over Taiwan has consistently driven Beijing s procurement decisions, and China can now bring significant capabilities to bear. The PLA Navy (PLAN) is now the largest navy in the world (as measured by the number of ships, although the United States continues to exceed it by tonnage), with 355 ships and submarines, and is set to grow by nearly 100 ships by the end of the decade.8 The PLA Air Force is the largest air force in the region and is rapidly catching up to Western air forces” and eroding U.S. advantages, according to the U.S. Department of Defense.9 The PLA has one thousand short-range ballistic missiles and six hundred medium-range ballistic missiles in its arsenal.10 China has also established an advanced integrated air defense system on its east coast that can cover Taiwan.11 The PLA is now turning its attention to addressing previous gaps that have persisted, such as anti-submarine warfare, while also rapidly developing information, cyber, and space and counterspace capabilities.12 Taiwan, however, is belatedly recognizing the need to dramatically rethink and invest in its defense. In 2017, its military leadership introduced the Overall Defense Concept(ODC), which aims to develop asymmetric approaches to fend off a Chinese invasion and calls for investing in a large number of smaller, cheaper, and more mobile weapons.23 Rather than seeking to defeat the PLA through attrition, ODC focuses on a decisive fight near Taiwans shores and the prevention of a successful PLA landing. Taiwan has steadily increased its defense budget in recent years, which is now the highest it has ever been in absolute terms.24 More important is using these funds to resource an asymmetric strategy, purchasing missiles, drones, and howitzers.25 There remain obstacles to ODC s implementation, however, and more traditional thinking could well make a comeback.26 All of this means that U.S. intervention on Taiwan s behalf would be a risky and costly proposition, as China can now challenge the United States across all domains and place U.S. aircraft, surface vessels (including aircraft carriers), and bases throughout the Indo-Pacific at risk. In addition, the United States would for the first time be fighting a nuclear-armed opponent with precision standoff weapons, extensive cyberwarfare capabilities, and the ability to target its satellites.27

#### China-Taiwan war goes nuclear. Deterrence is key.

Pettyjohn and Wasser 5-20-2022, \*senior fellow and director of the defense program at the Center for a New American Security, \*\*fellow in the defense program and co-lead of The Gaming Lab at the Center for a New American Security (Stacie and Becca, “A Fight Over Taiwan Could Go Nuclear,” *Foreign Affairs*, <https://www.foreignaffairs.com/articles/china/2022-05-20/fight-over-taiwan-could-go-nuclear/)//BB>

Russia’s invasion of Ukraine has raised the specter of nuclear war, as Russian President Vladimir Putin has placed his nuclear forces at an elevated state of alert and has warned that any effort by outside parties to interfere in the war would result in “consequences you have never seen.” Such saber-rattling has understandably made headlines and drawn notice in Washington. But if China attempted to forcibly invade Taiwan and the United States came to Taipei’s aid, the threat of escalation could outstrip even the current nerve-wracking situation in Europe. A recent war game, conducted by the Center for a New American Security in conjunction with the NBC program “Meet the Press,” demonstrated just how quickly such a conflict could escalate. The game posited a fictional crisis set in 2027, with the aim of examining how the United States and China might act under a certain set of conditions. The game demonstrated that China’s military modernization and expansion of its nuclear arsenal—not to mention the importance Beijing places on unification with Taiwan—mean that, in the real world, a fight between China and the United States could very well go nuclear. Beijing views Taiwan as a breakaway republic. If the Chinese Communist Party decides to invade the island, its leaders may not be able to accept failure without seriously harming the regime’s legitimacy. Thus, the CCP might be willing to take significant risks to ensure that the conflict ends on terms that it finds acceptable. That would mean convincing the United States and its allies that the costs of defending Taiwan are so high that it is not worth contesting the invasion. While China has several ways to achieve that goal, from Beijing’s perspective, using nuclear weapons may be the most effective means to keep the United States out of the conflict. China is several decades into transforming its People’s Liberation Army (PLA) into what the Chinese President Xi Jinping has called a “world-class military” that could defeat any third party that comes to Taiwan’s defense. China’s warfighting strategy, known as “anti-access/area denial,” rests on being able to project conventional military power out several thousand miles in order to prevent the American military, in particular, from effectively countering a Chinese attack on Taiwan. Meanwhile, a growing nuclear arsenal provides Beijing with coercive leverage as well as potentially new warfighting capabilities, which could increase the risks of war and escalation. China has historically possessed only a few hundred ground-based nuclear weapons. But last year, nuclear scholars at the James Martin Center for Nonproliferation Studies and the Federation of American Scientists identified three missile silo fields under construction in the Xinjiang region. The Financial Times reported that China might have carried out tests of hypersonic gliders as a part of an orbital bombardment system that could evade missile defenses and deliver nuclear weapons to targets in the continental United States. The U.S. Department of Defense projects that by 2030, China will have around 1,000 deliverable warheads—more than triple the number it currently possesses. Based on these projections, Chinese leaders may believe that as early as five years from now the PLA will have made enough conventional and nuclear gains that it could fight and win a war to unify with Taiwan. Our recent war game—in which members of Congress, former government officials, and subject matter experts assumed the roles of senior national security decision makers in China and the United States—illustrated that a U.S.-Chinese war could escalate quickly. For one thing, it showed that both countries would face operational incentives to strike military forces on the other’s territory. In the game, such strikes were intended to be calibrated to avoid escalation; both sides tried to walk a fine line by attacking only military targets. But such attacks crossed red lines for both countries, and produced a tit-for-tat cycle of attacks that broadened the scope and intensity of the conflict. For instance, in the simulation, China launched a preemptive attack against key U.S. bases in the Indo-Pacific region. The attacks targeted Guam, in particular, because it is a forward operating base critical to U.S. military operations in Asia, and because since it is a territory, and not a U.S. state, the Chinese team viewed striking it as less escalatory than attacking other possible targets. In response, the United States targeted Chinese military ships in ports and surrounding facilities, but refrained from other attacks on the Chinese mainland. Nevertheless, both sides perceived these strikes as attacks on their home territory, crossing an important threshold. Instead of mirror-imaging their own concerns about attacks on their territory, each side justified the initial blows as military necessities that were limited in nature and would be seen by the other as such. Responses to the initial strikes only escalated things further as the U.S. team responded to China’s moves by hitting targets in mainland China, and the Chinese team responded to Washington’s strikes by attacking sites in Hawaii. A NEW ERA One particularly alarming finding from the war game is that China found it necessary to threaten to go nuclear from the start in order to ward off outside support for Taiwan. This threat was repeated throughout the game, particularly after mainland China had been attacked. At times, efforts to erode Washington’s will so that it would back down from the fight received greater attention by the China team than the invasion of Taiwan itself. But China had difficulty convincing the United States that its nuclear threats were credible. In real life, China’s significant and recent changes to its nuclear posture and readiness may impact other nations’ views, as its nuclear threats may not be viewed as credible given its stated doctrine of no first use, its smaller but burgeoning nuclear arsenal, and lack of experience making nuclear threats. This may push China to preemptively detonate a nuclear weapon to reinforce the credibility of its warning. China might also resort to a demonstration of its nuclear might because of constraints on its long-range conventional strike capabilities. Five years from now, the PLA still will have a very limited ability to launch conventional attacks beyond locations in the “second island chain” in the Pacific; namely, Guam and Palau. Unable to strike the U.S. homeland with conventional weapons, China would struggle to impose costs on the American people. Up until a certain point in the game, the U.S. team felt its larger nuclear arsenal was sufficient to deter escalation and did not fully appreciate the seriousness of China’s threats. As a result, China felt it needed to escalate significantly to send a message that the U.S. homeland could be at risk if Washington did not back down. Despite China’s stated “no-first use” nuclear policy, the war game resulted in Beijing detonating a nuclear weapon off the coast of Hawaii as a demonstration. The attack caused relatively little destruction, as the electromagnetic pulse only damaged the electronics of ships in the immediate vicinity but did not directly impact the U.S. state. The war game ended before the U.S. team could respond, but it is likely that the first use of a nuclear weapon since World War II would have provoked a response. The most likely paths to nuclear escalation in a fight between the United States and China are different from those that were most likely during the Cold War. The Soviet Union and the United States feared a massive, bolt-from-the-blue nuclear attack, which would precipitate a full-scale strategic exchange. In a confrontation over Taiwan, however, Beijing could employ nuclear weapons in a more limited way to signal resolve or to improve its chances of winning on the battlefield. It is unclear how a war would proceed after that kind of limited nuclear use and whether the United States could de-escalate the situation while still achieving its objectives. AN OUNCE OF PREVENTION The clear lesson from the war game is that the United States needs to strengthen its conventional capabilities in the Indo-Pacific to ensure that China never views an invasion of Taiwan as a prudent tactical move. To do so, the United States will need to commit to maintaining its conventional military superiority by expanding its stockpiles of long-range munitions and investing in undersea capabilities. Washington must also be able to conduct offensive operations inside the first and second island chains even while under attack. This will require access to new bases to distribute U.S. forces, enhance their survivability, and ensure that they can effectively defend Taiwan in the face of China’s attacks. Moreover, the United States needs to develop an integrated network of partners willing to contribute to Taiwan’s defense. Allies are an asymmetric advantage: the United States has them, and China does not. The United States should deepen strategic and operational planning with key partners to send a strong signal of resolve to China. As part of these planning efforts, the United States and its allies will need to develop war-winning military strategies that do not cross Chinese red-lines. The game highlighted just how difficult this task may be; what it did not highlight is the complexity of developing military strategies that integrate the strategic objectives and military capacities of multiple nations. Moving forward, military planners in the United States and in Washington’s allies and partners must grapple with the fact that, in a conflict over Taiwan, China would consider all conventional and nuclear options to be on the table. And the United States is running out of time to strengthen deterrence and keep China from believing an invasion of Taiwan could be successful. The biggest risk is that Washington and its friends choose not to seize the moment and act: a year or two from now, it might already be too late.

### Modeling---Baltics

#### The Baltics lead on cyber policy.

Wierenga 22 [Louis Wierenga, Junior Research Fellow, Johan Skytte Institute of Political Studies, University of Tartu | Lecturer in International Relations, Department of Political and Strategic Studies, Baltic Defence College; 2022; "Cybersecurity and Hybrid Threats in the Digital Baltic States: A state of the art"; *Hybrid Threats in Baltics and Taiwan: Commonalities, Risks and Lessons for Small Democracies*; <https://www.baltdefcol.org/files/files/publications/Hybrid%20Threats_LIIA.pdf#page=58>; DL + KL]

Demonstrating leadership to allies:

If ever there was a time, as well as a concrete area for the Baltic states to showcase their strengths as small states, demonstrating leadership in the cyber and tech fields presents the perfect opportunity. Estonia has been the Baltic champion for cybersecurity and e-governance. Lithuania, and to a lesser extent Latvia have shown signs of catching up. Much like offline matters, the three Baltic states use opportunities to meet with US and EU leaders to highlight the dire security situation which the Transatlantic alliance faces from a resurgent Russia  – they know from experience and contemporary matters.

As the security of cyberspace is one of the acute questions of global politics this century33, cybersecurity and matters of digital warfare will be issues which merit pressing resolve, which is constantly changing. Being on the cutting edge will require countries to remain that way. While member of the United Nations Security Council for the first time, Estonia made cybersecurity a priority, along with the overall security of the region.34 As well, when a member of the UN Security Council, Estonia made it a point to align with the US and the UK to call Russia out over a cyberattack directed at Georgia.35

Latvia and Lithuania have also been active on such fronts. In 2021, Latvia signed an agreement with Poland which establishes a framework for cooperation between Latvia’s Military Information Technology Security Incident Team (MilCERT) and Poland’s National Cyber Security Center.36 Latvia is also taking the opportunity to reach out to the United States to discuss cybersecurity in the region.37 Lithuania has, as aforementioned, developed their own cyber center the RCDC, which is a bilateral LithuanianUS initiative.38

Conclusion

To conclude, the domain of cyberspace will be an arena for battle for the foreseeable future. All countries, governments, militaries will be faced with such threats, and the likelihood of businesses and private individuals being faced with such threats is high. The Baltic states are no strangers to such threats and have been leaders in facing up to them. Given the nature of threats faced and the manner in which the Baltics have faced up to them, it is safe to say that the Baltic states will continue to rise up to the challenges and keep up with the rapidly changing nature of cyber threats. However, the last point is the most persisting challenge any entity faces in cyberspace – the need to not only consistently keep up but remain steps ahead of adversaries. The bi- and multilateral agreements made as well as the leadership demonstrated, and the digital awareness can go a long way to not only meet contemporary and future challenges but serve as examples and demonstrate leadership. Cyber and hybrid threats are ominous, but on a positive note, the Baltic states have achieved many remarkable accomplishments in this field.

### Modeling---Middle East

#### The Middle East models.

Belmonte 7-20 [Nerea Belmonte, reporter; 7-20-2022; "The Baltic States, a defence model for the future of cyberwarfare"; Atalayar; https://atalayar.com/en/content/baltic-states-defence-model-future-cyberwarfare; KL]

The world is moving towards a digitised global society full of cyber opportunities. However, as a fully cyber-connected society, this future society will also have to cope with new patterns of conflict, such as cyber-attacks and hybrid warfare.

The Baltic countries - Estonia, Latvia, and Lithuania - which for years were under the control of the Union of Soviet Socialist Republics (USSR) and then forced to fight on the front line of digital warfare, have been forced to take the lead in this process of cyber-innovation. Moscow's attacks on the three pioneers of independence from the USSR have been a constant for years. And they have grown exponentially since the early 2000s.

The Estonian example

The Republic of Estonia was one of the Kremlin's first targets in 2007. Tallinn's decision to move the monument to the fallen Soviet soldiers of World War II from the centre of the capital to the 'Bronze Soldier' cemetery provoked a wave of cyber-attacks from Russia that lasted more than 20 days. Public and private organisations, ministries, banks, the media and even the parliament itself were affected by hundreds of hacker offensives.

"The government website normally receives between 1,000 and 1,500 hits a day; at the height of the attacks, in the first week of May, it received between 1,000 and 1,500 per second," explained defence spokesman Mikko Maddis at the time. "It blew up the system.

Fearing that the attack was just the prelude to a larger-scale cyber offensive, Estonia armoured itself. The small country shifted as many government services and systems as possible to new, private and secure networks, improving cyber security and protecting itself against the effects of digital warfare. This path also led Tallinn to transfer citizen services and the most basic government functions to blockchain technology.

Today, Estonia has become a country capable of dealing with almost any cyber threat; defined by The New Yorker as a "digital republic", its citizens have the opportunity to access virtually all available government services online, and its political and economic leaders to run it effectively from anywhere in the world.

Indeed, in 2014 Tallinn spearheaded the world's first e-residency programme, aiming to exceed 10 million residents by 2025. And while it has so far failed to add more than 85,000 residents, it has enabled more than 19,000 entrepreneurs to consolidate new digital companies that do not need to be physically present.

Russia's threat to Lithuania

The situation in neighbouring Lithuania, meanwhile, follows a similar fate. In the context of the Russian invasion of Ukraine, the country's main electricity company, Ignitis, suffered a few weeks ago what has been considered the biggest computer attack in the last decade. As the company itself reported in a press release, the blocking of its website and other electronic services was delayed for several hours until it could be repelled.

This attack, perpetrated according to Lithuanian sources by the Russian hacker group Killnet, was seen as part of Russian retaliation for the partial blockade of freight transport to the Kaliningrad Oblast. A strategic enclave for Moscow, located on the Baltic Sea halfway between Belarus and Poland, it allows Moscow to maintain a geopolitical sphere of influence in the region. "The offensive will continue until Lithuania lifts the block," the organisation told Reuters, "so far we have destroyed 1,652 web resources".

Russian-Ukrainian cyberwarfare

The war between Kiev and Moscow has also become another theatre of hybrid warfare. As the wave of Russian cyberattacks against Ukraine prior to the start of the invasion had already foreshadowed, the digital contest has also played an important role in the Kremlin's offensive; the massive distribution of malware, targeted attacks on highly critical infrastructure, and large-scale offensives against other Ukrainian websites (mainly through DDoS viruses, which make it impossible to access portals) have been just another weapon in Moscow's arsenal.

However, in such a scenario both sides have deployed their own "armies" and allies. While groups involved in ransomware-type attacks, such as Conti, have declared their support for the Russian regime, others, such as Anonymus, have declared war on Putin - conducting information exposure campaigns - and joined Kiev's "cyber army".

And in the future?

All this is evidence of the special importance of the cyber world on the international stage. Although the "Baltic laboratory" hardly seems exportable to other much larger and less technologically and digitally developed countries, most experts and analysts stress that it is necessary to know and monitor Estonian, Latvian and Lithuanian actions in their defence against Russian cyberattacks. The decisions taken by the small, once-Soviet states will serve as a guide to the characteristics and patterns of future cyber-conflicts.

According to technology expert Joseph Dana for the Syndication Bureau, it is now Middle Eastern countries - such as the United Arab Emirates and Israel - that are paying most attention to the features of these new wars, and to cyber-defence strategies. The reason for this is twofold. In addition to the large Emirati investment over the past decade to follow the Estonian model, "Emirati officials have also discussed the need to build a better cybersecurity infrastructure to safeguard the nation's knowledge economy".

Thus, many analysts have agreed that, should conflict break out between the Gulf states and Iran, cyberattacks would become a weapon of choice for both sides. Indeed, Israel and the Persian Islamic Republic have already exchanged several digital and technological offensives, and it is feared that these could extend beyond military infrastructure.

# Solvency Cards

#### The plan models NATO cybersecurity after the Baltics – empirically dissuades Russian attacks and secures US infrastructure.

Atalayar 7-20 [Atalayar, 7-20-2022, "The Baltic States, a defence model for the future of cyberwarfare", https://atalayar.com/en/content/baltic-states-defence-model-future-cyberwarfare, DOA: 7-20-2022 //ArchanSen]

The world is moving towards a digitised global society full of cyber opportunities. However, as a fully cyber-connected society, this future society will also have to cope with new patterns of conflict, such as cyber-attacks and hybrid warfare.

The Baltic countries - Estonia, Latvia, and Lithuania - which for years were under the control of the Union of Soviet Socialist Republics (USSR) and then forced to fight on the front line of digital warfare, have been forced to take the lead in this process of cyber-innovation. Moscow's attacks on the three pioneers of independence from the USSR have been a constant for years. And they have grown exponentially since the early 2000s.

The Estonian example

The Republic of Estonia was one of the Kremlin's first targets in 2007. Tallinn's decision to move the monument to the fallen Soviet soldiers of World War II from the centre of the capital to the 'Bronze Soldier' cemetery provoked a wave of cyber-attacks from Russia that lasted more than 20 days. Public and private organisations, ministries, banks, the media and even the parliament itself were affected by hundreds of hacker offensives.

"The government website normally receives between 1,000 and 1,500 hits a day; at the height of the attacks, in the first week of May, it received between 1,000 and 1,500 per second," explained defence spokesman Mikko Maddis at the time. "It blew up the system.”

Fearing that the attack was just the prelude to a larger-scale cyber offensive, Estonia armoured itself. The small country shifted as many government services and systems as possible to new, private and secure networks, improving cyber security and protecting itself against the effects of digital warfare. This path also led Tallinn to transfer citizen services and the most basic government functions to blockchain technology.

Today, Estonia has become a country capable of dealing with almost any cyber threat; defined by The New Yorker as a "digital republic", its citizens have the opportunity to access virtually all available government services online, and its political and economic leaders to run it effectively from anywhere in the world.

Indeed, in 2014 Tallinn spearheaded the world's first e-residency programme, aiming to exceed 10 million residents by 2025. And while it has so far failed to add more than 85,000 residents, it has enabled more than 19,000 entrepreneurs to consolidate new digital companies that do not need to be physically present.

#### Cooperation with Estonia is key – promotes cybersecurity for all of NATO

David Shedd 20, professor at the Patrick Henry College, former acting director of the Defense Intelligence Agency; and Ivana Stradner, Visiting Research Fellow at the American Enterprise Institute, J.S.D. from the University of California, Berkeley,8/11/2020, "Countering Russia’s Influence Operations in the Balkans," https://www.heritage.org/europe/commentary/countering-russias-influence-operations-the-balkans, RMax

Even the pandemic has the potential for fomenting political unrest.

In recent days, thousands of Serbs have taken to the streets to protest Serbian President Aleksandar Vucic’s announced strict curfew in response to a surge in Covid-19 cases. Many have pointed a finger at pro-Russia ultra-right groups and foreign intelligence services for fueling the violent riots.

Moscow denies any “Russian trace” in the unrest. Whether Russia is behind the violent protests in Belgrade remains to be seen. One thing is for certain. The Kremlin’s efforts to sow mayhem in the Balkans would not be new; this would merely be the latest attempt by a resurgent Russia to threaten Euro-Atlantic security and challenge the United States’ ability to defend its interests in Europe.

Russia is promoting its interests in the Western Balkans through the widespread use of disinformation and cyberwarfare. The U.S., however, isn’t helpless. It has an opportunity to obtain insights into these efforts and counter Russia's influence campaigns. It is time to confront Russia's strongman Vladimir Putin's cyber games before American interests are permanently damaged in the Balkans.

The U.S. and the E.U. have long been ambivalent about defining their interests in the Western Balkans. Russia has capitalized on these years of neglect and leveraged a power vacuum in the former Yugoslavia to gain economic and political influence. The region is now at the forefront of Russia's use of low-cost strategies to expand its global influence and undermine western interests.

Russian disinformation, aided by repeated cyberattacks on government institutions, was instrumental in the 2016 Moscow-sponsored coup attempt in Montenegro. In North Macedonia, Russia spread disinformation prior to the name-change referendum that finally enabled North Macedonia to join NATO. It also established hundreds of North Macedonia-based “troll factories," from which Russia pedaled fake news against the 2016 U.S. elections. Facebook recently banned troll farms from North Macedonia that pushed COVID-19 disinformation.

Moscow has also been investing in critical sectors in Croatia. With its strategy of fomenting political divisions, the Kremlin has been exploiting internal conflicts in Albania. In Bosnia and Herzegovina, disinformation campaigns have sown ethnic and religious discord, while promoting the secession of ethnic Serb regions from Bosnia. In response, the U.S. should encourage the transatlantic integration for Bosnia and Herzegovina, the Western Balkans’ most fragile country.

Russia has used state-sponsored media to promote nationalist and anti-Western narratives in Serbia, including the opening of a Sputnik office in Belgrade. Also,  Russian-run “Humanitarian Center” in Serbia is very close to the main NATO based in Kosovo (Camp Bondsteel). Some European and American officials fear that it serves as a base for the Kremlin intelligence-gathering activities to eavesdrop on U.S. interests in the Balkans.

Russia’s preeminent goals in the Balkans have been to refine their disinformation tactics and erode Western influence in the region, including in Croatia, Montenegro, North Macedonia and Albania, which are all NATO members. The West needs to aggressively respond to this Russian posture, including using a cyber-focused campaign to counter Russia's provocations.

For crafting such a strategy, the West should look to Estonia. After the 2007 Russian cyberattack on Estonian government institutions, Estonia became a global leader in cybersecurity and home to the NATO Cooperative Cyber Defense Centre of Excellence, which is a cyber-defense hub that supports member nations with cyber-defense expertise. A similar approach by the West would benefit the Western Balkans, where information and communication technology sector is the most promising and the fastest growing economic sector in the region. In Serbia alone, the I.T. sector generates more than 10% of GDP with a similar trend in other countries in the region, which have some of the highest numbers of outsourced I.T. workers per capita in Europe.

An American-led strategy should focus on creating a regional cyber-security infrastructure in the Western Balkans, modeled on Estonia's example. Given that countries in the Western Balkans share the same cyber-security threats from Russia and, more recently, from China, a regional hub for cybersecurity would allow states to cooperate among each other in cyber deterrence, attribution of attacks and collective countermeasures.

Several countries in the Western Balkans have joined NATO, but alliances are notoriously unreliable, especially among the smaller states. Countries in the Western Balkans need strong NATO and E.U. ties to withstand Russian influence. Cyber-security is one of the areas where they can strengthen their positions in allegiance with the western democracies.

The timing is excellent for the U.S. to establish a regional cyber-security hub in the Western Balkans. Immediate steps need to be taken to halt malign Russian influence. With elections approaching this year in the U.S., North Macedonia, Croatia and Montenegro, countries should continue cooperating to counter malicious Russian cyber activities.

The U.S. can learn more about Russian cyber tactics at the same time. One way to send a strong message would be to deploy a cyber-team to strengthen NATO’s countries’ cyber-capabilities in an effort to thwart future Russian network intrusions such as the one that was undertaken by Russian intelligence operators in Bulgaria in 2017.

Serbia, a key ally to Moscow in the region, remains the biggest obstacle to countering Russian influence. Serbia just had parliamentary elections boycotted by the opposition that resulted in Vucic's Serbian Progressive party winning a landslide victory and further strengthening his power. The close Russia-Serbian relationship can make it difficult to detect Russia's subversive activities.

Of all the Western Balkans countries, Serbia had the highest military expenditure in 2019, and President Vucic thanked Russia for making Serbia’s military 10 times stronger since NATO intervention in 1999. After Russia employed an S-400 missile system in Serbia for a military drill, the Pantsir S1 air-defense systems were delivered this past February, despite a looming U.S. sanctions threat.

Should Serbia continue obtaining Russian weapons, Washington should impose sanctions. Serbia must understand that its strategy of neutrality is unacceptable to the U.S., as are its claims to balance their interests among Russia, China and the West. The U.S. should remain solidly committed, leading efforts to solve the Kosovo dispute and wrest control of that narrative from Russia.

While variances in the national interests may complicate cooperation among the Western Balkan countries, they share similar vital objectives that make cooperation possible and even attractive under U.S. leadership. Among these are the historical fear of Russian domination and a desire for E.U. and NATO membership. A U.S.-led strategy with NATO country participation to enhance their cyber-capabilities will improve their security in countering nefarious Russian influence while enhancing cooperation between Balkan nations.

Moscow is determined to expand its influence in the Western Balkans, using cyber-warfare at the expense of U.S. and western interests. To prevent it, the U.S. should design a new strategy for the Western Balkans that demonstrates that the U.S. is committed to countering Russia's disruptive activities in the Western Balkans and beyond. The time for that response is now.

#### Estonia especially good at countering disinfo

* Cyberattacks in general too

Pernik 21 (Piret, is a researcher at the NATO Cooperative Cyber Defence Centre of Excellence (CCDCOE). She has researched cybersecurity strategic and policy aspects since 2013. She has published research reports and analyses on cyber resilience, military 5G security, cyber commands, and cyber defence training. She is also a co-editor of the volume Cyber Threats and NATO 2030: Horizon Scanning and Analysis, published by the CCDCOE. Her articles have been published in academic journals and she has written book chapters, as well as online commentaries. She holds an MA in Social Sciences from the University of Tallinn, and an MA in International Relations and European Studies from the Central European University, Budapest. “Cyber deterrence: A case study on Estonia’s policies and practice”, https://www.hybridcoe.fi/wp-content/uploads/2021/10/20211012\_Hybrid\_CoE\_Paper\_8\_Cyber\_deterrence\_WEB.pdf)LR

Estonia does not have a standalone policy of cyber deterrence, but strategic documents relating to national security, foreign policy and cybersecurity describe diverse components of cyber deterrence. Cybersecurity is deemed a part of foreign, security and defence policy, as well as domestic/internal security. It is also included in strategic documents and policies concerning digital modernization, technology, education and research, and so forth. The review and analysis of Estonia’s strategic documents associated with cybersecurity (presented in Annex I) shows that two concepts – cross-domain deterrence and cyber deterrence – play an important role in the government’s cybersecurity discourse. Three layers of deterrence – entanglement and norms, denial and punishment – are equally upheld. Generally speaking, the analysis demonstrates that in the Estonian national security discourse, deterrence by denial and punishment tend to be conceptualized in the context of national security and defence policy; entanglement and norms in the context of foreign policy and cyber diplomacy; and denial (domestic defence/resilience) in the context of digital and technology policies. In the latest strategy (2019–2022), cyber deterrence is referenced almost as frequently as in the 2014–2017 document, apart from the fact that cross-domain deterrence and military deterrence are not mentioned. Rather, concerns about challenges relating to digital modernization and technology policies come to the fore in this strategy. The last column of Table 2 provides examples of how a deterrence tool has been implemented. Table

Description automatically generated To strengthen its cyber diplomacy capacity, Estonia established a position in 2018 for an ambassador-at-large for cybersecurity. Estonia is one of the leaders among the Baltic and Nordic countries when it comes to cyber diplomacy. It has been a member of the UN Group of Governmental Experts for many years, and is also a leader in cyber diplomacy education for foreign diplomats.35 As a member of the UN Security Council in 2020– 2021, in June 2021 Estonia organized for the first time in the Council’s history an open meeting on cybersecurity, where it raised the issue of state behaviour in cyberspace in the context of international peace and security.36 Since 2008, Estonia has hosted the NATO Cooperative Cyber Defence Centre of Excellence (CCDCOE), which sponsors the publication of world-renowned scholarly works on international law applicable to cyberspace – the Tallinn Manuals 1.0 (2013), 2.0 (2017), and the forthcoming volume 3.0.37 Deterrence by denial, conceptualized in Estonia primarily as domestic defence/resilience measures, is foundational for the country’s cybersecurity posture.38 Deterrence in this area includes a full spectrum of activities prescribed in the national cybersecurity strategies, in cybersecurity legislation and other relevant ministerial regulations. Some of the resilience-related objectives have remained constant since 2008, such as applying measures to harden networks (for example, standards, risk analysis and management tools, incident response, raising awareness, building cybersecurity capacity and competence, to name a few).39 In June 2021, Estonia published its first national information security standard entitled E-ITS, which is a guideline for public and private network owners and operators to ensure minimum security standards.40 The Estonian Information System Authority regularly alerts stakeholders and the general public to cyber threats, vulnerabilities and exploits, and helps them to protect their networks. These activities contribute to deterrence by denial by increasing the ability to protect networks and recover from cyber incidents. Public attribution can be regarded as a tool for deterrence.46 Indeed, among Estonian experts, public attribution is regarded as a primary tool of cyber deterrence.47 As noted by scholars, one aim of public attribution is the act of norm-setting – that is, establishing “the rules of the road” and subsequently enforcing appropriate behaviour in cyberspace (response measures).48 In a similar manner, the Estonian government holds that “public statements on attribution can be made, with the aim of increasing accountability in cyberspace and emphasising the importance of adhering to international law obligations and norms of responsible state behaviour”.49 The Estonian Ministry of Foreign Affairs subscribes to the opinion that “public attribution […] allows states to send clear messages and shape expectations that malicious cyberspace operations will not be tolerated” and “it is necessary to send a message that harmful cyberspace operations are not part of acceptable state behaviour”.50 In other words, Estonia directly links public attribution to setting cyber norms, thus connecting deterrence by entanglement and norms to legal consequences, namely deterrence by punishment. According to this view, Estonia supports public attribution and collective measures “where possible” and “public attribution and messaging are tools for deterring and responding […] but also for raising wider awareness”.51 To support collective public attribution and to hold violators responsible, Estonia actively contributes to EU and NATO cyber deterrence discussions, and belongs to the US-led international cyber deterrence initiative.52 Based on the Estonian case study, a policy recommendation for EU and NATO countries is to apply a three-layered deterrence model.73 First, EU and NATO countries should participate in entanglement and norms measures such as cyber diplomacy and capacity-building globally. Second, they should invest more in denial measures and, third, jointly develop policies for punitive response options, including developing public attribution procedures to enable quick attribution, and systematically implementing sanctions regimes. It would be feasible to establish memoranda of understanding, and operational- and technical-level frameworks to radically improve information- and intelligence-sharing. Participation in cyber defence and crisis management exercises should be open to like-minded NATO partner countries. Joint bilateral cyberspace operations likewise contribute to mutual trust-building and information-sharing, and increase parties’ operational and technical competence.74 Operational- and technical-level joint activities should be regularly practised among allies and with like-minded partners as they contribute to deterrence by denial. Given that NATO’s cyber With regard to deterrence by denial, Estonia, together with other EU and NATO countries, should develop a zero trust security strategy and architecture.75 Zero trust is a cybersecurity paradigm that treats networks as untrusted, and that moves defences from static, network-based perimeters to focus on users, assets, and resources. It assumes that there is no implicit trust granted to user accounts or assets in any network segment (including a corporate local area network), and applies authentication and authorization before a session is established.76 While deterrence might work at the high end, novel security principles should be implemented by governments because deterrence is not sufficient to deter cyberattacks. Estonia’s public attribution guidelines serve as a blueprint for other countries to attribute cyberattacks and impose meaningful costs. A sharper focus on responses to high- and low-end cyberattacks should be developed in the future along with concrete deterrence actions and tools for individual 75 For example, the US government has released a strategy, architecture and maturity model that the US federal government agencies will implement: ‘Moving the U.S. Government Towards Zero Trust Cybersecurity Principles’, The White House, https://zerotrust.cyber.gov/. 76 Scott Rose, Oliver Borchert, Stu Mitchell and Sean Connelly, ‘Zero Trust Architecture SP 800-207’, August 2020, NIST, https://csrc.nist.gov/publications/detail/sp/800-207/final. 77 ‘Nye, Deterrence and Dissuasion in Cyberspace’, p. 62. sectors and target types. For example, deterrence tools can differ for diverse targets: internet voting and e-health systems would be targeted by different cyber threat actors that have political or criminal motives, and the same tool is not effective across all actors. Estonia’s forms of cyber deterrence are not effective individually, nor every time, but when implemented together in a whole-of-society approach, and systematically over a longer period of time, it is likely that many malicious cyberattacks can be deterred. As Joseph Nye pointed out, deterrence tools “can complement one other in affecting actors’ perceptions of the costs and benefits of particular actions”.77 Certainly, one cannot deter all cyberattacks – especially those conducted as part of malicious influencing campaigns below the threshold of the use of force – however, it is possible to reduce the number and effect of strategic cyberspace operations. It is likely that punitive responses may deter hostile actors from conducting similar attacks in the future. It will remain to be seen whether the EU and NATO can deter cyberattacks both above and below the threshold of an armed attack better in the future when they apply systematically stronger punitive responses.

#### Baltic cyberspace alliance solvency advocate

Libicki 19. Martin C. Libicki is an American scholar and Professor at the Frederick S. Pardee RAND Graduate School in Santa Monica, California; “For a Baltic Cyberspace Alliance?”; 2019 11th International Conference on Cyber Conflict; <https://ccdcoe.org/uploads/2019/06/Art_01_For-a-Baltic-Cyberspace-Alliance.pdf> //BY

* AT: Germany PIC

3. NATO AS A CYBERSPACE ALLIANCE The logic of international alliance is that bigger is usually better when defending against threats.5 Although the size of the alliance and the need for consensus can complicate warfighting,6 the concept of a common defense means that an adversary faces the combined militaries of multiple countries. In a world in which attackers are dissuaded by the prospect that united countries will interpose their forces between attackers and those being defended, the premise that more is better makes intuitive sense. But combat in cyberspace does not really benefit from economies of scale. Within a country, adding more offensive cyber warriors often means lowering the qualifications (at least initially, and perhaps in the long term) for what is, by nature, an inherently elite profession. This means not only that diminishing returns set in, but that the activities of the good-but-not-great can well tip off the other side. So tipped, the other side can improve its defenses in ways that are specific (e.g., vulnerabilities are patched after having been discovered) and general (i.e., a shift occurs in the tradeoff between security and cost/convenience). Correspondingly, the contribution of additional operators is limited. When these operators come from other countries, their contribution is further vitiated unless these countries operate seamlessly. Within an intelligence-sharing alliance (e.g., the Five Eyes), additional members do add heft (each country, for instance, can employ relationships that it has developed with communications companies around the world). Once seams intrude – and these seams are larger within NATO than within the Five Eyes – the level of coordination is less and the prospects for interference (e.g., two countries seeking access to the same target system) are greater. When it comes to defense, the arguments that vitiate the benefits mass are different but similar. A large percentage of all cyber defense efforts requires looking after specific systems. Adding allies adds more systems to defend. This hardly helps defenders of existing systems.7 Although there are defense activities where adding countries may help – e.g., intelligence fusion, collective learning, and forensics – none of these really requires a military alliance, and some of the contributors for these three efforts live in the private realm. Alliances also express their weight through deterrence policies. In the Cold War, the United States deterred attacks by the Soviet Union on NATO allies with a nuclear threat: certainly, if the attacks involved nuclear weapons, and quite possibly if the attack involved overwhelming conventional force. In recent years the U.S. deterrence policy in cyberspace has been notionally extended to a NATO deterrence policy. Unfortunately, U.S. deterrence policy for attacks on the homeland is already an uncertain thing – and extending it adds further uncertainties. There are, for instance, serious questions about what constitutes a cyberattack serious enough to merit retaliation and what the form of retaliation would be; the United States has used sanctions in response to malign cyberspace activities, but there is little evidence that sanctions have deterred Russia, Iran, or North Korea.8 NATO’s retaliation capabilities – which are largely US retaliation capabilities (plus some UK capabilities) – are even less likely to be brought into play if the target of a cyberattack were European. In the five years prior to North Korea’s hack of Sony – which the United States did respond to – South Korea suffered far worse depredations with no U.S. response.9 4. AND WHY IS THE NATO GROUPING NOT THE OBVIOUS ONE? Yet Europeans lean on NATO; in large part, because it already exists and therefore does not need to be invented. But NATO is a military alliance, while cyberspace is essentially a conduit for information,10 hence generally dominated by the community that deals with information qua intelligence. And the existence of the Five Eyes coalition only underlines this point: working relationships among that coalition in the information domain are tighter than they are in the information domain across the NATO alliance. And two of the Five Eyes are not even in NATO. In other words, the real coalition is not doing Europe (the UK excepted) in particular that much good. This matters, because the primary cyber war threat to Europe is from Russia, and the primary targets of Russian coercion are in European countries that face Russia. Two of the countries that face the gravest threats are not even in NATO. Correspondingly, a Baltic cyberspace alliance would have a limited ambit: members would cooperate on defense and aver that a cyberattack on one is an attack on all. In practice, were such an arrangement made, the alliance would have its own definition of what constitutes an “attack”; it might include social media manipulation. A cyberspace alliance, as such, would have three facets but lack one. The first facet is defense: each country would putatively participate more vigorously in those cyber defense activities that benefit from scale, as noted: threat intelligence, forensics, lessons learned. With very large cyberattacks, they could offer mutual aid for systems restoration. The second facet is defense by deterrence. It would require a consensus on what constitutes an actionable offense in cyberspace, notably the type and severity; what responses are appropriate (e.g., to an attack on the local power grid); and what kind of capability is required to retaliate in cyberspace. One rationale for responding in cyberspace is that less forceful options, such as alliance-wide sanctions, are likely to be even weaker than U.S. sanctions are. Conversely, threatening kinetic responses – given the lack of nuclear weapons among proposed alliance members – lacks credibility thanks to Russia’s escalation dominance. The third facet would consist of offensive cyberspace operations used for coercive or, more likely, counter-coercive purposes or for retaliation against grave non-cyber offenses (e.g., the Skripal poisonings11). By contrast, cyberspace operations in support of kinetic operations (e.g., taking a SAM site offline while a NATO sortie flies overhead) would fall outside such an alliance because kinetic operations fall to NATO; if individual members carried out tactical cyberattacks, they would fall under NATO auspices (or their own fights). 5. CHARACTERISTICS AND ADVANTAGES OF A BALTIC CYBERSPACE ALLIANCE What are the characteristics and advantages of such an alliance to its member countries? First, the alliance, limited to cyberspace, would invariably focus on Russia, despite having to tend to other threats (e.g., from China’s commercially-motivated cyberespionage) and despite the possibility that alliance members would probably be diplomatic in public about the alliance’s purpose. Russia’s cyberspace threats are malevolent, politically-directed, and often part of a larger campaign to sow disorder and facilitate coercion. NATO countries, as a whole, are not entirely focused on Russia, these days: those in North America pay as much attention to China;12 those near the Mediterranean tend to look southward. Second, such an alliance would include currently neutral countries, notably Sweden and Finland. Both countries punch above their weight, in cyberspace operations13 and information operations14 respectively. This raises the question: why don’t such countries just enter NATO? To be sure, roughly half the citizens in both countries would like to – but the other half fear, justifiably, a neuralgic Russian reaction if they did (Finland’s accession could put troops along miles of Russian borders). Although Russians would likely react badly to the formation of a Baltic cyberspace alliance, they would have a more difficult time summoning images of jackbooted soldiers while doing so. For Sweden and Finland, the cyberspace alliance could serve as a halfway house. If the Russian threat eases, their entry into NATO can be indefinitely postponed (in the unlikely event that the Russian cyberspace threat disappears, they can leave or the cyberspace alliance might wither away). If the Russian threat persists or worsens, these two countries will have had more practice interoperating with NATO countries, thereby easing their way into an alliance that spans the conventional domains of warfare. Third, a cyberspace alliance would be a mechanism to get Germany to become more involved – or, more to the point, take leadership – in defending Europe against Russia. The current contribution of German military spending (1.2 percent of GDP) to the common defense of NATO is modest. Germany, nevertheless, remains Europe’s largest economy, and would constitute roughly half of the weight of any Baltic cyberspace alliance. Germany has also stepped up smartly in developing its Cyber and Information Domain Service. Its manning, if plans hold,15 would constitute 7.5 percent of Germany’s total force level (13,500 out of 180,000);16 its spending would be 6.3 percent of Germany’s military (41.5 billion Euro) budget.17 By way of contrast, USCYBERCOM’s end-strength goal of 6,000 compares to 1.3 million military personnel in the overall U.S. military – less than a tenth as much concentration on cyberspace. Granted, this is not an apples-to-apples comparison: Germany’s end strength includes electronic warfare battalions; USCYBERCOM’s end-strength does not. But, even after adjustments, Germany’s commitment to fighting in cyberspace, relative to its overall military strength, looks more substantial than the U.S. commitment. Furthermore, a German focus on cyberspace (vis-à-vis kinetic elements of military power) is, again, less likely to engender a neuralgic reaction from Russia (no jackboots, etc.) but does put Russia on notice that its maneuvers in cyberspace have not gone unnoticed and will be resisted by those best placed to resist them. The advantage of such an alliance to its members is that they put the power of all in service of each. This should give Russians second thoughts about their use of cyberspace for offensive purposes – although it may also initially goad them into carrying out operations against the non-NATO countries (Sweden and Finland) to inhibit their participation in such an alliance. Russia’s doing so, conversely, could very well reinforce the value to today’s neutral countries of having others to lean on when facing Russia. The countries in this alliance would be self-selected by virtue of their concern over Russian activities in cyberspace. By contrast, a unified and meaningful NATO response to Russian provocations has to surmount the objections of countries that reserve some sympathy for Russia (Hungary and Greece come to mind). Fourth, this would give NATO competition in the alliance business. Arguably, this would weaken NATO – and is thereby a disadvantage. But competition can also be good: it persuades competitors to listen to their clients (customers, audience, etc.) and induces them to innovate in order to retain their standing. Otherwise, secure in the knowledge that their position is unassailable, they risk becoming sluggish and unresponsive – and when they fall or come apart, it is often “first slowly and then all at once”.18 Thus, when offering cyber security or countering cyberattacks, relevant countries can ask the institutions of NATO and also those of the Baltic cyberspace alliance what each of them can do – each knowing that they are competing both against Russia’s malign influence and the other’s benign influence. But competition can also raise problems: an institutionally aggressive cyberspace alliance may seek greater influence by stretching the definition of a cyberattack: e.g., to include electronic warfare, interference with space operations, and sabotage of or attacks on information infrastructures. 6. ADVANTAGES FOR THE UNITED STATES The most basic advantage is that it makes Europeans more responsible for their own defense, albeit in just this one domain. In the 1980s, for example, three neutral countries – Switzerland, Sweden, and Finland – spent far higher proportions of their income on national defense than most European NATO allies did.19 The “free rider” problem is, if anything, worse today. It may be that much more difficult to persuade European countries to arm themselves if, when such arms have to be used, it would be under a war effort led by the United States. The return of Russia as an aggressive power, since roughly late 2013, may not have been internalized by European countries, concerned as they are with internal fissures – many of which, ironically, were deliberately exacerbated by Russia’s information warfare campaign. And the U.S. pivot to Asia, while more advertised than practiced, would necessarily mean a shift in U.S. resources that would otherwise be available for Europe. But in cyberspace, countries in a Baltic cyberspace alliance would be pooling their resources under either their own individual command (as befits an activity so highly linked to intelligence) or, at least under the command of Europeans. And with the United States not in such an alliance, there is much less of a “free rider” problem (even if Germany would be roughly half the alliance, countries such as Sweden, Finland, and Estonia punch above their weight in this domain). The downside of the upside is akin to the owner of a hammer being persuaded that every problem is a nail: if given a choice between responding to hostile actions in the kinetic world and responding in cyberspace, the latter may be seen as particularly attractive because it relies on tools the alliance can wield themselves rather than tools largely wielded by the United States. Another advantage for the United States is that such an alliance may complicate Russia’s cyber war efforts – largely by increasing the uncertainty that Russian efforts may be met with reprisals: the odds of retaliation from either the United States (as the premier cyberspace power of NATO) or from the Baltic cyberspace alliance will be higher than the odds of retaliation from each of them. This is particularly true for those cyberattacks that leave multiple victims: NotPetya, as an example, levied costs in the hundreds of millions of dollars from Merck and Federal Express (both U.S.-headquartered corporations) and from Maersk (headquartered in Denmark). The raised odds for a response may arise from meeting credibility thresholds (the United States may be wary and the Baltic cyberspace alliance less so or vice versa), attribution thresholds (the United States may have confidence and the Baltic cyberspace alliance may not or vice versa), and damage thresholds (the United States may recognize a higher threshold to warrant its retaliation if the effects of the cyberattack fall primarily on Europeans). Both the United States and the Baltic cyberspace alliance may retaliate but against different targets.20 An associated benefit is that if the modus operandi of whatever cyberspace operations ensue from NATO (that is, in practice, from the United States or the UK) and the Baltic cyberspace alliance are sufficiently similar, it may not be clear to Russia who struck back. This would complicate counter-retaliation targeting (and threats), in anticipation of which retaliation may be more likely, and the prospect thereof more credible. To be fair, attack-retaliation cycles in cyberspace remain loose: the closest example of a retaliatory cyberattack was the late 2012 DDOS campaign against U.S. banks by an Iran that had, two years earlier, discovered that its nuclear program had been set back by the Stuxnet worm. Attack-retaliation-counter-retaliation cycles are even more nthorder relationships. Furthermore, Russia may have the SIGINT or HUMINT to make its own attribution – or it may not care and may conclude that the Baltic cyberspace alliance is an arm of NATO despite the former having neutral countries in it; indeed, it may see all opposing alliances as arms of the United States, facts notwithstanding.

#### Mutual Cooperation is key

Horchakova 2022, Veronika Horchakova Mykolas Romeris University, European and International Business Law program, Master’s degree student(“STRENGTHENING THE TRANSATLANTIC PARTNERSHIP: CHALLENGES AND OPPORTUNITIES FOR THE BALTIC STATES” https://repository.mruni.eu/bitstream/handle/007/18311/Teisines\_minties\_svente-97-107.pdf?sequence=1)

In conclusion, taking into account the current geopolitical situation and the number of commitments in the international arena, the Baltic States are likely to remain strong US allies and important US security partners in Europe. Analysts believe that close cooperation between the United States and the Baltic States will continue for the foreseeable future in areas such as efforts to deter potential Russian aggression, the future of NATO, energy security, and socioeconomic issues. As long as there are objective fears of peace demolition, NATO is interested in deepening cooperation with like-minded countries. There is still work to be done within the Baltic region to strengthen resistance to Russian propaganda and maintain sovereignty and determination towards pro-European standards in the socio-economic field. This work will follow, for instance, the example of banning Russian propaganda in the media. To achieve this, the Baltic States will likely continue to rely on the United States for leadership on foreign policy and security issues. This can be seen from current partnership programs devoted to enhancing defence power and providing training and an educational practicum. This reliance is not only from the side of the Baltic region; it is seen as a reciprocal one. For instance, there are climate change issues where Lithuania can share its experience and the best approaches to green ecology with the United States, and the US may be more eager to cooperate with Lithuania. Moreover, in terms of geopolitics, the United States should try to defeat China’s attempts to collaborate with US allies on the same issues. On successfully implementing and finalising those partnership activities, further steps will be taken to proceed with cooperation. In short, the United States’ commitment to Baltic security is part of the US commitment to European security, and the former would not and cannot exist without the latter. As new challenges are emerging, more efforts should be made to guarantee these commitments, thus strengthening transatlantic ties concerns building this partnership, reinforcing power, and preventing threats. This attitude undoubtedly appears to be beneficial for both sides.

#### Baltics need more cyber defense

* Recut for civ-mil cp lol

Veebel 17 (Viljar Veebel is a researcher and consultant who has been researching in the University of Tartu, The Estonian School of Diplomacy and The Tallinn Technological University. “Baltic States and Cyber Deterrence: Taking or Losing Initiative against Russia”https://www.fpri.org/article/2017/01/baltic-states-cyber-deterrence-taking-losing-initiative-russia/)LR

Based on Russia’s strategy in Ukraine and Georgia, elements of “cyber warfare” will likely play an important role in future Russian conflicts. Russia carried out similar or even more advanced attacks during the Russian-Georgian conflict in 2008 and the Ukrainian conflict from 2013. In Georgia, attackers combined targeted denial-of-service attacks (DDOS) with military action to impede strategic communications and to create panic among civilians. During the Russian-Ukrainian conflict, Russia’s strategy has also focused on disinformation and psychological warfare through online media, massive trolling on social media, and even attacks on mobile phone operators. In contrast to their NATO counterparts, Russia’s cyber and propaganda units have shown great independence from moral considerations or legal hesitation, using every opportunity to compromise the Baltic states and NATO. Considering Russia’s current ambitions in Ukraine, the Baltic states are not likely the most important targets of Russian cyber attacks. However, as the “cyber war” from 2007 showed, they are vulnerable. **If transatlantic security priorities change after Brexit and Trump’s election, the Baltic countries may come under considerable pressure again.** From Cyber Defense to Cyber Deterrence Following its experience in 2007, Estonia has become a pioneer in international cyber security. Fortunately, contrary to military capabilities and power games, the size of a country does not matter much here. A cyber war’s battlefield is the whole world, and quality, initiative, and position are often more important than quantity. Waiting for the opponent’s first moves and relying only on defense does not bode well for success. Additionally, standardized and comfortable administrative procedures in combination with the highest possible compliance with international law offer little advantage against an opponent using a more flexible command model and selective approach to international law. The Baltic countries should strive to stay a step ahead of Russia. To achieve this goal, they must combine the resources and the knowledge of both the private and the public sector, guaranteeing more flexibility when countering cyber threats**.** First**,** cyber deterrence and cyber defense must be re-conceptualized and distinguished **from one another**. The Baltic states all too often understand cyber defense as a passive instrument that produces effective deterrence by itself. Thus, they focus mainly on reactive and defensive measures, with the status quo as the best possible outcome in regional cyber confrontation. As part of a re-conceptualization of cyber deterrence, it is also crucial to better understand Russia in terms of its fears and weaknesses, and a wider circle of specialists should contribute to cyber deterrence. More awareness of Russian technological capabilities, motives, and recent practices is also necessary. Second, the organizational structure and procedures of cyber defense units need to combine the best practices from the public, private, and military sectors, each with advantages and limits. The command chain must focus on results as much as possible, with automatic procedures and flexible power delegation in critical situations. Currently, army practices and rules dominate the logic of decision-making and resource distribution. However, the military rotation cycle, rank-based roles, commitment to manuals, the tendency to avoid innovation, strong limits for investments and procurements, and intolerance to failures do not contribute to success in cyber conflicts. Speed, flexibility, expertise, and new solutions are crucial there. Third, globalization and limited legal regulation of cyber security and deterrence must be fully exploited. There is no need to limit preparation and actions to traditional state boundaries, “best-practices” of the public sector, moral considerations, and legal hesitation. Cyber security units can and should have cells outside NATO territories, employ private contractors, and use unexpected retaliation tactics. Taking these actions can create the best possible deterrence against Russia’s model of aggressive hybrid warfare. Governments must equip their cyber units with the best possible resources in advance, and these units should have permission to test their tactics and tools and tolerance for failure during the development of these procedures. To start, more visible power, initiative, and agility will help to create effective deterrence against Russia. In practical terms, cyber defense action needs to follow a pre-emptive mentality because if Russian forces attack first, they might disable further defense or counterattack capabilities. By limiting cyber defense only to self-defense in the spirit of best moral and legal considerations, the Baltic states and NATO in general give Russia a comfortable zone of action. NATO voluntarily restricts itself from efficient strategies and warfare. Crimea was a clear sign for the West that in a hybrid war restricting oneself to a reactive role and “playing a Russian game” without innovation and initiative will lead to defeat. Baltic states have very little time and a lot to do: these countries and NATO should not merely focus on spending 2% of GDP on defense, but be more specific about the capabilities required to achieve the compulsory level of traditional and cyber deterrence. Goals, red lines, and success markers require more clarity. After Brexit in the UK, and the U.S. presidential elections, **the Baltic states must further develop their cyber capabilities, especially cyber deterrence. Preserving peace may depend on it.**

### Say yes

#### Say yes.

Gilliam and Van Wie 22 [Colonel John B. Gilliam, U.S. Army Armor Officer, senior executive fellow at the Strobe Talbott Center on Strategy, Security, and Technology at the Brookings Institution; Major Ryan C. Van Wie, U.S. Army Infantry Officer, international affairs instructor in the Social Sciences Department at the United States Military Academy; 3-2022; "Feasible U.S. steps to strengthen NATO deterrence in the Baltics and Poland"; The Brookings Institution; https://www.brookings.edu/wp-content/uploads/2022/03/FP\_20220322\_nato\_deterrence\_gilliam\_van\_wie.pdf; KL]

While most of our recommendations focus on the U.S. Army, it is worth continuing to press NATO to make mobility improvements and investments that ultimately will enhance the alliance’s effectiveness in the Baltics. As suggested in the Atlantic Council’s report “Moving Out,” the U.S. should pressure NATO members to invest in dual-use infrastructure such as Rail Baltica, expand strategic lift capacity and the prepositioning of equipment, digitize border-crossing and customs procedures, and build cyber resilience.90 By focusing NATO members’ investment on non-kinetic capabilities with benefits to civil society, the likelihood of European nations agreeing to do so is far more likely than arguing for the purchasing of advanced weaponry or additional force structure. As a component of this line of effort and as recommended in “Moving Out,” NATO members should purchase additional heavy equipment transporters such as the British M1070F, which is compliant with European regulations.91 Such an investment would help U.S. and NATO forces arrive to the Baltics quicker in a crisis. Finally, NATO members, such as Poland and Germany, should consider purchasing flatbed railcars and even forming some type of modest rail battalion under a NATO structure akin to what Russia utilizes. Doing so would fill an identified shortage of rail cars across Europe and ensure their availability in a crisis.92 Having dedicated and trained military rail personnel to operate the trains would also enable timely and effective movement.

#### Countries want defensive military modernization.

Klein et al. 19 [Colonel Robert M. Klein, Senior Military Fellow in the Center for Strategic Research (CSR), Institute for National Strategic Studies, at the National Defense University; Lieutenant Commander Stefan Lundqvist, Ph.D., Researcher and Faculty Board Member at the Swedish Defence University (SEDU); Colonel Ed Sumangil, USAF, Senior Military Fellow in CSR; Ulrica Pettersson, Ph.D., assigned to SEDU, Adjunct Faculty Member at Joint Special Operations University; 11-2019; "Baltics Left of Bang: The Role of NATO with Partners in Denial-Based Deterrence"; *Strategic Forum* 301, Institute for National Strategic Studies, National Defense University; https://inss.ndu.edu/Portals/68/Documents/stratforum/SF-301.pdf; KL]

The NATO goal should be to knit partners together in a networked system of advanced command, control, communications, computers, intelligence, surveillance, and reconnaissance (C4ISR), targeting, precision-guided munitions, airborne early warning capabilities, integrated air defenses, maritime domain awareness, undersea surveillance, and standoff capabilities such as cruise and ballistic missiles. This networked system-of-systems approach has come to define the contemporary revolution in military affairs. Policy analysts James Thomas and Evan Montgomery have dubbed these “mini A2/ AD complexes.”25 The current willingness of key Allies and partners—particularly those in the Baltic region—to modernize their militaries makes it a favorable time for NATO to implement such a defensive concept. Therefore, providing partners with additional enabling capabilities to round out their defensive formations may prove critical. To enhance area denial, NATO needs additional mobile and survivable long-range precision-strike capabilities such as the Army Tactical Missile System (ATACMS) and Highly Mobile Artillery Rocket System. The Army is currently developing DeepStrike, a next-generation missile for these systems that doubles the firepower and can engage targets at distances up to 499 km, including the ability to hit moving targets on land and at sea.26 To counter Russian tactical missiles, cruise missiles, drones, and advanced aircraft, additional NATO and partner countries should procure the Patriot and other surface-to-air missile defense systems.

#### Ukraine makes it uniquely popular.

Tol et al. 22 [Jan van Tol, Senior Fellow at the Center for Strategic and Budgetary Assessments. Prior to his retirement from the Navy in 2007, Captain van Tol served as special advisor in the Office of the Vice President. He was a military assistant to Andrew W. Marshall, the Secretary of Defense’s Principal Advisor for Net Assessment, from 1993–1996 and 2001–2003. At sea, he commanded three warships, two of which, USS O’Brien (DD-975) and USS Essex (LHD-2), were part of the U.S. Navy’s Forward Deployed Naval Forces based in Japan. Captain van Tol’s analytic work has focused mainly on long-range strategic planning, naval warfare, military innovation, and wargaming. He holds a B.A. in Philosophy and Logic from the University of Massachusetts/Amherst and a M.S. in Operations Research from the Naval Postgraduate School, and graduated with distinction from the College of Naval Command and Staff at the U.S. Naval War College; Christopher Bassler, Senior Fellow at the Center for Strategic and Budgetary Assessments, where he researches technology & innovation, joint aerospace capabilities, maritime operating concepts, and overall U.S. & allied military strategies. He served as a civilian in the Department of Defense, for both the Departments of the Navy and the Air Force, as an engineer, designer, strategist, and advisor. His previous assignments include the F-35 Joint Program Office, the Office of the Chief of Naval Operations (OPNAV) in the Pentagon, the Office of Naval Research, and the Naval Surface Warfare Center, Carderock Division. He has worked in various capacities to enhance capabilities and interoperability across all warfighting domains, in many technology areas, and with key allies and partners on five continents, including NATO for both the capabilities and the S&T Organisation. He was awarded two U.S. Patents. Dr. Bassler received two U.S. Navy Meritorious Civilian Service Awards, from the U.S. Secretary of the Navy and the Chief of Naval Research. His degrees include a Ph.D. in Aerospace Engineering from Virginia Tech; a M.A. in Security Policy Studies from the George Washington University Elliott School of International Affairs; and a Diploma in Strategy & Innovation from the University of Oxford, Saïd Business School; Katherine Kjellström Elgin, Fellow at the Center for Strategic and Budgetary Assessments. She brings rigorous research to policy discussions and has held positions in both academic and policy organizations. Prior to joining CSBA, she served as a DAAD Post-Doctoral Fellow at the Foreign Policy Institute of Johns Hopkins School of Advanced International Studies (SAIS), where she wrote and published on grand strategy, great power relations, U.S. defense strategy, European security, and alliance management. Dr. Elgin has also worked at the Brookings Institution and with the Long Term Strategy Group in Washington, D.C. In 2018, she served as a visiting fellow at the Institute for Security & Development Policy in Stockholm, Sweden. Dr. Elgin earned her Ph.D. in Public Affairs (Security Studies) from Princeton University’s School of Public & International Affairs. At Princeton, she served as the director of the Center for International Security Studies’ Strategic Education Initiative, leading the university’s program for educating and mentoring students with an interest in national and international security; Tyler Hacker, Analyst at the Center for Strategic and Budgetary Assessments. His work focuses on U.S. defense strategy, future warfare, and great power competition. Prior to joining CSBA, Tyler was an analyst at the Congressional Research Service, where he conducted research on topics in defense logistics. Tyler previously served as a field artillery officer in the United States Army in Germany, where he participated in NATO operations and exercises in Poland, Romania, and the Baltic states. He has also completed internships at the U.S. Army War College and the American Enterprise Institute. He holds a B.A. in International Studies from Virginia Military Institute and an M.A. in Security Studies from Georgetown University; 2022; "Executive Summary"; *Deterrence and Defense in the Baltic Region: New Realities*, Center for Strategic and Budgetary Assessments (CSBA); https://csbaonline.org/uploads/documents/CSBA8312\_(Deterrence\_Defense\_Baltic)\_web.pdf; LR + KL]

The NATO posture “reset” announced by Secretary Stoltenberg, if properly and promptly executed, could greatly reduce the potential for a Russian fait accompli against the Baltic states as well as deter aggression against other NATO states on the eastern border. Presently it is broadly supported among the NATO member states because of the ongoing Russia-Ukraine war and its accompanying atrocities. However, depending on the evolution of the conflict, the enthusiasm and willingness of some member states may flag over time or individual member state priorities may start to shift. For any reset to be successful, there must be genuine burden-sharing among all member states, whether on the eastern front or not, until NATO’s “reset” is fully implemented.

## Prodicts

### Prodict---Brookings

#### Brookings is #1.

TTCSP 21 [James G. McGann, Ph.D. Senior Lecturer, International Studies Director, Think Tanks and Civil Societies Program, The Lauder Institute, University of Pennsylvania; 1-28-2021; "2020 Global Go To Think Tank Index Report"; *TTCSP Global Go To Think Tank Index Reports*; https://repository.upenn.edu/cgi/viewcontent.cgi?article=1019&context=think\_tanks; KL]

THINK TANK OF THE YEAR – TOP THINK TANK IN THE WORLD

Center of Excellence for 2017-2020

Brookings Institution (United States)

### Prodict---Carnegie

#### Carnegie is the best\* think tank worldwide.

\*Actually Brookings is #1, but the #1 think tank from past years doesn’t get ranked for the next three years

TTCSP 21 [James G. McGann, Ph.D. Senior Lecturer, International Studies Director, Think Tanks and Civil Societies Program, The Lauder Institute, University of Pennsylvania; 1-28-2021; "2020 Global Go To Think Tank Index Report"; *TTCSP Global Go To Think Tank Index Reports*; https://repository.upenn.edu/cgi/viewcontent.cgi?article=1019&context=think\_tanks; KL]

2020 Top Think Tanks Worldwide (US and non-US)

Table 3

1. Carnegie Endowment for International Peace (United States)

### Prodict---CEPA

#### CEPA is the 21st best think tank in the world.

TTCSP 21 [James G. McGann, Ph.D. Senior Lecturer, International Studies Director, Think Tanks and Civil Societies Program, The Lauder Institute, University of Pennsylvania; 1-28-2021; "2020 Global Go To Think Tank Index Report"; *TTCSP Global Go To Think Tank Index Reports*; https://repository.upenn.edu/cgi/viewcontent.cgi?article=1019&context=think\_tanks; KL]

2020 Best Regional Studies Centers (Free Standing)

Table 53

1. Center for Strategic and International Studies (CSIS) (United States)

2. Organization for Social Science Research in Eastern and Southern Africa (Ethiopia)

3. Fundação Getúlio Vargas (FGV) (Brazil)

4. Asian Development Bank Institute (Japan)

5. Azerbaijan Center for Economic and Social Development (Azerbaijan)

6. Brookings Institution (Qatar)

7. Chinese Academy of Social Science (China)

8. East West Center (United States)

9. Australia Institute for Regional Security (Australia)

10. Middle East Institute (United States)

11. Center for the Study of African Economies (United Kingdom)

12. Carnegie Endowment for International Peace Moscow Center (Russia)

13. German Institute of Global and Area Studies (Germany)

14. African Technology Policy Studies Network (Kenya)

15. Comisión Económica para América Latina y el Caribe (Chile)

16. Fundación para el Análisis y los Estudios Sociales (Spain)

17. Atlantic Council (United States)

18. Food, Agriculture and Natural Resources Policy Analysis Network (South Africa)

19. African Economic Research Consortium (Kenya)

20. Institute of Southeast Asian Studies (Singapore)

21. United States Center for European Policy Analysis (United States)

22. George C. Marshall European Center for Security Studies (Germany)

23. Mitvim Israeli Institute for Regional Foreign Policies (Israel)

24. Hungarian Center for Economic and Regional Studies (Hungary)

25. International Institute for Iranian Studies, FKA Arabian Gulf Center (Saudi Arabia)

26. National Bureau of Asian Research (United States)

27. Russian Institute for the U.S. and Canadian Studies (Russia)

28. Russian Institute for Oriental Studies (Russia)

29. Indonesian Economic Research Institute for ASEAN and East Asia (Indonesia)

30. Mercator Institute for China Studies (MERICS) (Germany)

31. Polish Center for Eastern Studies (Poland)

32. Carnegie Endowment for International Peace India Center (India)

33. Regional Centre for Strategic Studies (Sri Lanka)

34. Carnegie Endowment for International Peace China Center (China)

35. Ghana Center for Democratic Development (Ghana) 36. Russian Institute of Europe (Russia)

37. India Center for the Study of Developing Societies (India)

38. Sheikh Saud bin Saqr Al Qasimi Foundation for Policy Research (United Arab Emirates)

39. Hammurabi Center for Research and Strategic Studies (Iraq)

40. Kyrgyzstan Institute for Regional Studies (Kyrgyzstan)

41. Carnegie Endowment for International Peace Europe (Belgium)

42. Caribbean Natural Resources Institute (West Indies)

43. Organization for Social Science Research in Eastern and Southern Africa (Ethiopia)

#### The Regional Studies category ranks objective and unbiased think tanks.

TTCSP 21 [James G. McGann, Ph.D. Senior Lecturer, International Studies Director, Think Tanks and Civil Societies Program, The Lauder Institute, University of Pennsylvania; 1-28-2021; "2020 Global Go To Think Tank Index Report"; *TTCSP Global Go To Think Tank Index Reports*; https://repository.upenn.edu/cgi/viewcontent.cgi?article=1019&context=think\_tanks; KL]

Best Regional Studies Policy Research Center (Free-Standing, Not University-Affiliated): Think Tanks honored in this category are independent of government or university affiliation and are self-governing institutions. These institutions are autonomous and produce quality research that is objective and unbiased.

### Prodict---Prodict of Prodict

#### That’s out of 11,000 think tanks ranked by thousands of experts.

TTCSP 21 [James G. McGann, Ph.D. Senior Lecturer, International Studies Director, Think Tanks and Civil Societies Program, The Lauder Institute, University of Pennsylvania; 1-28-2021; "2020 Global Go To Think Tank Index Report"; *TTCSP Global Go To Think Tank Index Reports*; https://repository.upenn.edu/cgi/viewcontent.cgi?article=1019&context=think\_tanks; KL]

Introduction The 2020 Global Go To Think Tank Index (GGTTI) marks the fifteenth year of continued efforts by the Think Tanks and Civil Societies Program (TTCSP) at the University of Pennsylvania to acknowledge the important contributions and emerging global trends of think tanks worldwide. Our initial effort to generate a ranking of the world’s leading think tanks in 2006 was a response to a series of requests from donors, government officials, journalists and scholars to produce regional and international rankings of the world’s preeminent think tanks. Since its inception, our ongoing objective for the GGTTI report is to gain an understanding of the role think tanks play in governments and civil societies. Using this knowledge, we hope to assist in improving the capacity and performance of think tanks around the world.

Since 2006, the ranking process has been refined and streamlined, and the number and scope of the institutions and individuals involved has steadily grown. The process, as in past years, relies on a shared definition of public policy research and analysis and engagement organizations, a detailed set of selection criteria and an increasingly open and transparent nomination and selection process. As part of the nominations process, all 11,175 think tanks catalogued in TTCSP’s Global Think Tank Database were contacted and encouraged to participate in the nomination and ranking process. Over 44,992 journalists, policymakers, public and private donors, and functional and regional area specialists on the TTCSP listserv were invited to participate and over 3,974 fully or partially completed the nomination and ranking surveys. Finally, a group of peers and experts was asked to help rank and review the public policy research Centers of Excellence for 2020.

To refine and validate the generated ranking lists, TTCSP assembled Expert Panels comprised of hundreds of members from a wide variety of backgrounds and disciplines. Additionally, new media—the website and social media presence—helped us communicate and disseminate information about criteria for this year’s Index to a wider audience (please see “Methodology and Timeline” for the complete set of nomination and ranking criteria and “Appendices” for a detailed explication of the ranking process). Given the rigor and scope of the nomination and selection processes, the rankings produced thus far have been described as the insider’s guide to the global marketplace of ideas.

As a final note, we would like to remind you that the data collection, research and analysis for this project, as in previous years, were conducted without the benefit of field research, a budget or staff. Despite these limitations, we are confident in the quality and integrity of the findings given the number of peers and experts from around the world who have taken the time to participate in the process.

We are confident that the peer nomination and selection process, as well as the work of the international Expert Panels, have enabled us to create the most authoritative list of highperformance think tanks in the world. Still, efforts to streamline and perfect the process are ongoing. We are continually seeking ways to enhance the process and welcome your comments and suggestions. We further encourage you to provide the names and contact information for prospective expert panelists for functional and regional areas covered by the Index. Thank you for your continued support of TTCSP and of the annual Global Go To Think Tank Index. We hope our efforts to highlight the important contributions and emerging global trends of think tanks worldwide will foster insightful discussions and debates on the present and future roles of these vital institutions.

### Prodict---GMF

#### It’s the 155th think tank in the world! Chart for reference.

TTCSP 21 [James G. McGann, Ph.D. Senior Lecturer, International Studies Director, Think Tanks and Civil Societies Program, The Lauder Institute, University of Pennsylvania; 1-28-2021; "2020 Global Go To Think Tank Index Report"; *TTCSP Global Go To Think Tank Index Reports*; https://repository.upenn.edu/cgi/viewcontent.cgi?article=1019&context=think\_tanks; KL]

2020 Top Think Tanks Worldwide

(US and non-US) Table 3 1. Carnegie Endowment for International Peace (United States) 2. Bruegel (Belgium) 3. Fundação Getúlio Vargas (FGV) (Brazil) 4. Center for Strategic and International Studies (CSIS) (United States) 5. French Institute of International Relations (IFRI) (France) 6. Chatham House (United Kingdom) 7. RAND Corporation (United States) 8. Japan Institute of International Affairs (JIIA) (Japan) 9. Peterson Institute for International Economics (PIIE) (United States) 10. Wilson Center, FKA Woodrow Wilson International Center for Scholars (United States) 11. Center for American Progress (CAP) (United States) 12. International Institute for Strategic Studies (IISS) (United Kingdom) 65 13. Heritage Foundation (United States) 14. Fraser Institute (Canada) 15. Konrad-Adenauer-Stiftung (KAS) (Germany) 16. Korea Development Institute (KDI) (Republic of Korea) 17. Friedrich-Ebert-Stiftung (FES) (Germany) 18. China Institutes of Contemporary International Relations (CICIR) (China) 19. Council on Foreign Relations (CFR) (United States) 20. Observer Research Foundation (ORF) (India) 21. Carnegie Endowment for International Peace Middle East Center (Lebanon) 22. Centre for European Policy Studies (CEPS) (Belgium) 23. African Centre for the Constructive Resolution of Disputes (ACCORD) (South Africa) 24. Asian Development Bank Institute (ADBI) (Japan) 25. Clingendael, Netherlands Institute of International Relations (Netherlands) 26. Carnegie Endowment for International Peace Moscow Center (Russia) 27. Cato Institute (United States) 28. Institute for International Political Studies (ISPI) (Italy) 29. Elcano Royal Institute (Spain) 30. Centre for International Governance Innovation (CIGI) (Canada) 66 31. Urban Institute (United States) 32. Korea Institute for International Economic Policy (KIEP) (Republic of Korea) 33. Institute of World Economy and International Relations (IMEMO) (Russia) 34. Danish Institute for International Studies (DIIS) (Denmark) 35. Stiftung Wissenschaft und Politik (SWP) (Germany) 36. Barcelona Centre for International Affairs (CIDOB) (Spain) 37. Consejo Argentino para las Relaciones Internacionales (CARI) (Argentina) 38. Chinese Academy of Social Sciences (CASS) (China) 39. American Enterprise Institute for Public Policy Research (AEI) (United States) 40. Razumkov Centre (Ukraine) 41. Institute for Defence Studies and Analyses (IDSA) (India) 42. German Development Institute (DIE) (Germany) 43. Stockholm International Peace Research Institute (SIPRI) (Sweden) 44. Belfer Center for Science and International Affairs (United States) 45. LSE IDEAS (United Kingdom) 46. Atlantic Council (United States) 47. Urban Institute (United States) 48. Istituto Affari Internazionali (IAI) (Italy) 67 49. Singapore Institute of International Affairs (SIIA) (Singapore) 50. Carnegie Endowment for International Peace (China) 51. Amnesty International (AI) (United Kingdom) 52. Rasanah: International Institute for Iranian Studies (Saudi Arabia) 53. Transparency International (TI) (Germany) 54. International Crisis Group (ICG) (Belgium) 55. Royal United Services Institute (RUSI) (United Kingdom) 56. Development Research Center of the State Council (DRC) (China) 57. Centre for Economic Policy Research (CEPR) (United Kingdom) 58. China Institute of International Studies (CIIS) (China) 59. Al-Ahram Center for Political and Strategic Studies (ACPSS) (Egypt) 60. Fedesarrollo (Colombia) 61. Center for Social and Economic Research (CASE) (Poland) 62. German Council on Foreign Relations (DGAP) (Germany) 63. Kiel Institute for the World Economy (IfW) (Germany) 64. Center for China and Globalization (CCG) (China) 65. Norwegian Institute of International Affairs (NUPI) (Norway) 66. Institute of Economic Affairs (IEA) (United Kingdom) 68 67. East Asia Institute (EAI) (Republic of Korea) 68. Bonn International Center for Conversion (BICC) (Germany) 69. African Economic Research Consortium (AERC) (Kenya) 70. Libertad y Desarrollo (LyD) (Chile) 71. Australian Institute for International Affairs (AIIA) (Australia) 72. Food, Agriculture and Natural Resources Policy Analysis Network (FANRPAN) (South Africa) 73. Overseas Development Institute (ODI) (United Kingdom) 74. Asia Society Policy Institute (ASPI) (United States) 75. Institute of Foreign Affairs and National Security (IFANS) (Republic of Korea) 76. Lowy Institute for International Policy (Australia) 77. Centre for European Reform (CER) (United Kingdom) 78. Institute of Development Studies (IDS) (United Kingdom) 79. Turkish Economic and Social Studies Foundation (TESEV) (Turkey) 80. Wilfried Martens Centre for European Studies (WMCES), FKA Centre for European Studies (Belgium) 81. Institute of International and Strategic Studies (IISS), FKA Center for International and Strategic Studies (China) 82. World Economic Forum (WEF) (Switzerland) 83. Centre for Civil Society (CCS) (India) 69 84. European Union Institute for Security Studies (EUISS) (France) 85. South African Institute of International Affairs (SAIIA) (South Africa) 86. Centre for Strategic and International Studies (CSIS) (Indonesia) 87. Centre for Conflict Resolution (CCR) (South Africa) 88. Centro de Implementación de Políticas Públicas para la Equidad y el Crecimiento (CIPPEC) (Argentina) 89. Heinrich-Böll-Stiftung (HBS) (Germany) 90. Association for Liberal Thinking (ALT) (Turkey) 91. Demos (United Kingdom) 92. European Centre for International Political Economy (ECIPE) (Belgium) 93. Timbro (Sweden) 94. Bangladesh Institute of Development Studies (BIDS) (Bangladesh) 95. Centro de Estudios Públicos (CEP) (Chile) 96. Shanghai Institutes for International Studies (SIIS) (China) 97. Institute of Southeast Asian Studies (ISEAS) (Singapore) 98. Civitas: Institute for the Study of Civil Society (United Kingdom) 99. Centro de Divulgación del Conocimiento Económico para la Libertad (CEDICE) (Venezuela) 100. Kenya Institute for Public Policy Research and Analysis (KIPPRA) (Kenya) 101. Institute of Defence and Strategic Studies (IDSS) (Singapore) 70 102. Centre for Public Policy Studies (CPPS) (Malaysia) 103. African Technology Policy Studies Network (ATPS) (Kenya) 104. Fundación Alternativas (Spain) 105. Unirule Institute for Economics (China) 106. Polish Institute of International Affairs (PISM) (Poland) 107. Hudson Institute (United States) 108. Center for Free Enterprise (CFE) (Republic of Korea) 109. Institute for National Security Studies (INSS) (Israel) 110. Indian Council for Research on International Economic Relations (ICRIER) (India) 111. Energy and Resources Institute (TERI) (India) 112. Our Hong Kong Foundation (China) 113. IMANI Center for Policy and Education (Ghana) 114. Potsdam Institute for Climate Impact Research (PIK) (Germany) 115. National Bureau of Economic Research (NBER) (United States) 116. Institute for Security Studies (ISS) (South Africa) 117. Institute for International Policy Studies (IIPS) (Japan) 118. Centre for Independent Studies (CIS) (Australia) 119. EUROPEUM Institute for European Policy (Czech Republic) 71 120. EGMONT – The Royal Institute for International Relations (Belgium) 121. European Policy Centre (EPC) (Belgium) 122. Fundação Armando Alvares Penteado (FAAP) (Brazil) 123. Free Market Foundation (FMF) (South Africa) 124. Moscow State Institute of International Relations (MGIMO) (Russia) 125. Council for the Development of Social Science Research in Africa (CODESRIA) (Senegal) 126. Lithuanian Free Market Institute (LFMI) (Lithuania) 127. Instituto Ecuatoriano de Economía Política (IEEP) (Ecuador) 128. Facultad Latinoamericana de Ciencias Sociales (FLACSO) (Costa Rica) 129. Adam Smith Institute (ASI) (United Kingdom) 130. Center for Policy Studies (CPS) (Hungary) 131. Regional Centre for Strategic Studies (RCSS) (Sri Lanka) 132. Istituto Bruno Leoni (IBL) (Italy) 133. Center of Analysis of International Relations (AIR Center) (Azerbaijan) 134. Mercatus Center (United States) 135. Centro de Estudio de la Realidad Económica y Social (CERES) (Uruguay) 136. Hoover Institution (United States) 137. National Institute for Defense Studies (NIDS) (Japan) 72 138. Development Alternatives (DA) (India) 139. Gulf Research Center (GRC) (Saudi Arabia) 140. Economic Policy Research Centre (EPRC) (Uganda) 141. Centre for Liberal Strategies (CLS) (Bulgaria) 142. Delhi Policy Group (India) 143. Chicago Council on Global Affairs (United States) 144. Ifo Institute – Leibniz Institute for Economic Research (Germany) 145. Finnish Institute of International Affairs (FIIA) (Finland) 146. Inter-American Dialogue, Washington (United States) 147. Consejo Mexicano de Asuntos Internacionales (COMEXI) (Mexico) 148. Hellenic Foundation for European and Foreign Policy (ELIAMEP) (Greece) 149. Fondazione Eni Enrico Mattei (FEEM) (Italy) 150. Friedrich Naumann Foundation for Freedom (FNF) (Germany) 151. Center for Economic and Social Development (CESD) (Azerbaijan) 152. Institución Futuro (Spain) 153. World Resources Institute (WRI) (United States) 154. México Evalúa Centro de Analisis de Politicas Publicas & CIDAC (Mexico)

155. German Marshall Fund of the United States (GMF) (United States)

156. Acton Institute for the Study of Religion and Liberty (United States) 157. Initiative for Development and Global Governance (IDGM) (France) 158. Centro Euro-Mediterraneo sui Cambiamenti Climatici (CMCC) (Italy) 159. New America Foundation (United States) 160. Center for Global Development (CGD) (United States) 161. Ethiopian Development Research Institute (EDRI) (Ethiopia) 162. Centro de Análisis e Investigación (Mexico) 163. Organization for Social Science Research in Eastern and Southern Africa (OSSREA) (Ethiopia) 164. Centro de Investigaciones Económicas Nacionales (CIEN) (Guatemala) 165. Copenhagen Consensus Center (Denmark) 166. Israel-Palestine: Creative Regional Initiatives (IPCRI) (Israel) 167. Centro Studi Internazionali (Ce.S.I.) (Italy) 168. Institute of Statistical, Social and Economic Research (ISSER) (Ghana) 169. Cambodia Development Resource Institute (CDRI) (Cambodia) 170. Caucasus Institute for Peace, Democracy and Development (CIPDD) (Georgia) 171. Centre for Land Warfare Studies (CLAWS) (India) 172. Centre for Geopolitical Studies (GEOPOLITIKA) (Lithuania) 173. Centre for Policy Research (CPR) (India) 74 174. Fundación Libertad (Argentina)

Prodict---Prodict

# Add Ons

### Add-On---Creative Economy

#### The Baltics solves the creative economy.

Štreimikienė and Kacˇerauskas 20 [Dalia Štreimikienė, Faculty of Public Governance and Business, Mykolas Romeris University, Vilnius, Lithuania; Tomas Kacˇerauskas, Faculty of Creative Industries, Department of Philosophy and Cultural Studies, Vilnius Gediminas Technical University; 7-12-2020; "The creative economy and sustainable development: The Baltic States"; *Sustainable Development* 28; https://onlinelibrary.wiley.com/doi/pdf/10.1002/sd.2111?casa\_token=EeQAAx6bpU0AAAAA:CGi0Bs9eKTmtNvAW2-q2G86MhIK-SbxCS9\_n6F-znAUBXEcHZJR9JJlsuM1IpLQ-WRZ58xduSkFyKQ; KL]

The creative economy is one of the fastest developing sectors in the global economy, providing income growth, new jobs and export earnings. In addition to economic benefits that flow from cultural and creative industries, the aforementioned contribute to resolving issues of sustainable urban development, as well as contributing to the 2030 Agenda, which is the main initiative of the United Nations. Although it is acknowledged by scholars that creativity promotes inclusive social progress and empowers people to take responsibility for their own economic, social and personal development and encourages innovation, which contributes significantly to sustainable growth, there is lack of empirically tested results. The article aims to analyse the linkages between the implementation of sustainable development goals achieved by countries, and the development of the creative economy in such countries. The empirical data were collected for comparison of creativity and sustainability indexes by reference to the case study of the Baltic States. Policy implications were provided based on the research conducted. The study found that Estonia is the best performing country in terms of measures of creativity and assessments of that country's creative economy. Furthermore, Estonia is the most sustainable country, and has achieved the greatest progress in implementing sustainable development goals of any of the Baltic States. All of the environmental indicators for Latvia, and taking into account Lithuania's economic indicators place these two countries at the same level in terms of sustainability.

#### Extinction.

Saltmarshe and Pembroke 20 [Ella Saltmarshe, co-founder of the Long Time Project; Beatrice Pembroke, Executive Director Culture at King's College London; 7-14-2020, dated with Wayback Machine; "Why do we need to get long-term?"; The Long Time Project; https://www.thelongtimeproject.org/; KL]

Short-termism is rapidly becoming an existential threat to humanity. Short-term mindsets and structures across business, government and society are threatening our collective future.

The next few decades will be pivotal for the billions who have yet to be born. If we act wisely, humanity will survive; the Earth may remain habitable for at least a billion years; what has occurred so far could be a tiny fraction of possible human history and achievement. But, there is a darker alternative too. One where we don’t make the necessary changes in time and where we wipe ourselves out as a species, taking many others with us.

The tunnel vision of short-term thinking is leading to decisions that might mean we are only left with a short term as a species.

We’ve started The Long Time Project as we believe three things:

Our capacity to care about the future is crucial to our ability to preserve it. We need to feel an emotional connection to future generations.

Developing longer perspectives on our existence will change the way we behave in the short term.

Art and culture will be crucial to cultivating long-term attitudes and behaviours. They are foundational in shaping our collective direction of travel, from the kinds of laws we make, to the technology we develop, to the way we think about our role in shaping the future.

### Institutions

#### Baltic State Utility to US

Banka 2022, (Andris Banka , Journal of Transatlantic Studies volume 20, pages161–183 (2022), Published 4/5/2022 “Neither reckless nor free-riders: auditing the Baltics as US treaty allies” https://link.springer.com/article/10.1057/s42738-022-00096-3)

A great deal of scholarly literature has treated Baltic States’ physical proximity to Russia as their Achilles heel. The conventional wisdom holds that due to the force imbalance in the region, which heavily favours the Russian side, Baltic republics are hard to defend territories.Footnote82 While this assumption is certainly valid, there is, however, a flip side to this predicament. Situated at a geopolitical crossroads, these small nations are in an advantageous position to produce valuable insights into Kremlin’s statecraft. As James Carafano suggests: “To a major power, a country’s greatest asset might be its map coordinates rather than the size of its arsenal or bank account”.Footnote83 Similarly, Brands and Feaver have noted that some of the most valued US intelligence assets stem from allied partners “geographical capability” and “proximity to the theater of interest”.Footnote84 Lacking in material power resources, the Baltic States, within the past decade, have made a concerted effort to set up “knowledge hubs” that excel in analysing their much larger eastern neighbour. Having been subjected to Russian-directed gray zone tactics for decades, the Baltics have amassed valuable regional expertise. Testifying before the US Committee on Foreign Affairs, a prominent Russia-observer explained: “They [the Baltics] see things that we don’t see. They can go to places that we don’t go. They understand things that we don’t in cyber and intelligence”.Footnote85 Retired Lieutenant General Ben Hodges, who commanded the US Army Europe, concurs by emphasizing that the Baltic republics, due to their location, “know more what is happening in Russia, than any American will ever know”.Footnote86 Indeed, the Baltics fill in critical gaps in fields such as cyberwarfare, intelligence gathering, and disinformation, actively sharing this “know-how” with their US counterparts. The following details such contributions The Republic of Estonia was the first known victim of a state-directed cyberattack. The 2007 incident, widely attributed to the Russian Federation, for weeks incapacitated Estonian governmental structures. Somewhat paradoxically, in the long run, the event turned out to have a positive impact as it propelled the nation of 1.3 million people to treat the cyber domain as an intricate part of its national security. Subsequently, the country set up the Tallinn-based NATO Cooperative Cyber Defence Centre of Excellence. According to the Estonian President Kersti Kaljulaid, this was a smart way for a small country to demonstrate its contributions to allies.Footnote87 Understanding that it has little to offer in hard-power deliverables, Estonian leadership chose instead to focus on the cyber domain. In the words of Kaljulaid’s predecessor, Toomas Ilves, the IT field served as “the great equalizer”, allowing a small nation to contribute considerably more than one “would expect by looking at the map, population, and GDP per capita”.Footnote88 Today, Estonia has a well-established reputation among its peers as the lead authority for devising cybersecurity-related solutions. When it comes to countering cyber threats, Tallinn and Washington have forged a close bilateral relationship on various departmental levels. In 2020, the two governments set up a joint cyber-threat intelligence-sharing platform.Footnote89 In addition, the US Army and Estonia’s Ministry of Defence entered into an agreement for collaborative research on cyber defence matters.Footnote90 Such joint initiatives have already borne fruit. In the run-up to the 2020 US Presidential election, in order to learn more about Russian hacking methods, the USA dispatched its cyber force operatives to Estonia.Footnote91 For the USA, this allowed to observe the work of Kremlin-linked agents and bolster its own election defences. Commenting on this deployment, US Deputy Assistant Secretary of Defense for Cyber Policy pointed out: “Cyber is a team sport—when it comes to halting threats from cyberspace, no one can go it alone”.Footnote92 Such operations illustrate how small states can amplify the reach of the USA and effectively complement its capabilities. Estonian authorities have regularly received praise for the provision of such services. James Mattis, US Secretary of Defense in the Trump administration, upon meeting his Estonian counterpart underscored that Washington highly appreciates Estonian leadership in this new area of competition, and that its positive example speaks to the fact that the size of the country does not necessarily determine its contributions to collective security.Footnote93 In a similar vein, NATO Secretary-General Jens Stoltenberg has spoken highly of Estonia for its efforts in training and educating NATO military staff.Footnote94 After being the first victim of a Russian-linked cyberattack, Estonian leadership managed to turn the incident into a certain asset. By studying its lessons and building resilience, it gradually emerged as the lead cyber-knowledge exporter. For many, Russia’s abilities to effectively plant disinformation campaigns overseas came into sharper focus during the 2016 US presidential election. For the Baltics, however, such malign interference and attempts to sow societal divisions were hardly anything new. Lawmakers in the region have been sounding the alarm about it ever since regaining independence in the early 1990s. However, it was only in 2014 that Latvia opened the NATO Centre of Excellence devoted to the exploration of such issues. Its central analytical focus is on tracking and analysing Russia’s digital footprint. Since its establishment, the research institution has produced innovative studies regarding information-warfare efforts employed by Kremlin-linked actors and experimental takes on societal vulnerabilities. Such analysis has often been shared with the US government via testimonies before the US Senate Select Committee on Intelligence and briefings with the US military staff.Footnote95 Commenting on the centre’s work, a senior US Congressman pointed out that because of their “first-hand experience with the Soviet Union and Putin’s Russia”, the Baltics have become “a valuable source of insight” for the US government.Footnote96

#### Trust in institutions – extinction.

Tisdall 22 [Simon Tisdall is a foreign affairs commentator. He has been a foreign leader writer, foreign editor and US editor for the Guardian, 1-9-2022, "The epic struggle for America’s soul is just getting started", Guardian, https://www.theguardian.com/commentisfree/2022/jan/09/the-epic-struggle-for-americas-soul-is-just-getting-started, DOA: 7-20-2022 //ArchanSen]

A new USA Today/Suffolk University poll found eight in 10 Republicans, Democrats and independents are worried about the future of American democracy. But they disagree over the causes – and who’s to blame: 85% of Democrats call the Capitol Hill rioters “criminals”; two-thirds of Republicans believe “they went too far but had a point”.

“Only free and fair elections in which the loser abides by the result stand between each of us and life at the mercy of a despotic regime,” warns Harvard law professor Laurence Tribe. But increasingly, for today’s politicians, honourable defeat is a wholly foreign concept.

This chronic loss of institutional trust and credibility, also tainting a politicised, conservative-dominated supreme court, reflects a society more openly riven by longstanding cultural, racial and religious animosities – and one in which income, wealth and health inequalities are growing. These divisions are in turn wilfully exacerbated by rightwing broadcast and online media, bloggers and internet trolls.

A Republican party mostly in thrall to Trump’s lies, delusions and conspiracy theories is creating a world of “alternative facts”, says columnist Thomas Friedman. If they succeed in replacing truth, “America isn’t just in trouble. It is headed for what scientists call ‘an extinction-level event’”.

Jedediah Britton-Purdy, a Columbia law professor, is similarly apocalyptic. “One thing Democrats and Republicans share is the belief that, to save the country, the other side must not be allowed to win … Every election is an existential crisis,” he wrote.

“We should stop underestimating the threat facing the country,” a grim New York Times editorial thundered last week. “January 6 is not in the past; it is every day. It is regular citizens who threaten election officials, who ask ‘when can we use the guns?’, who vow to murder politicians who dare to vote their conscience. It is Republican lawmakers scrambling to make it harder for people to vote and subvert their will if they do. It is Trump who stokes the flames of conflict.” Democracy, it said, was in “grave danger”.

Systemic violence that overwhelms conventional politics may be near at hand. “We are closer to civil war than any of us would like to believe,” says Barbara Walter, a California politics professor.

No one is talking about a remake of the 1861-65 US civil war. Instead, as in Ukraine or Libya, an “open insurgency”, as defined by Walter, would probably involve (at least initially), disparate militias and their supporters pursuing forms of asymmetrical warfare – typically terrorist acts, bombings, assassinations, kidnappings. That said, worrying echoes of Confederate-era secessionism are once again heard in Texas and elsewhere.

When the warlike rhetoric of Charlottesville-style paramilitary white supremacists, the high nationwide incidence of gun ownership and, for example, worries about far-right cells within the US military are factored in, civil war scenarios do not appear so implausible.

“Only a spark is needed, one major domestic terrorist event that shifts the perception of the country,” analyst Stephen Marche wrote last week. Marche quotes a military history professor and Iraq war veteran, Col Peter Mansoor, who tells him: “It would not be like the first civil war, with armies manoeuvring on the battlefield. I think it would very much be a free-for-all, neighbour on neighbour, based on beliefs and skin colours and religion. And it would be horrific.”

### China

#### retag---5G cyber is the new battlefield, mutual cooperation between US-NATO with the Baltics key to combat China and Russia

Wierenga 22 (Louis Wierenga Junior Research Fellow, Johan Skytte Institute of Political Studies, University of Tartu | Lecturer in International Relations, Department of Political and Strategic Studies, Baltic Defence College. “Cybersecurity and Hybrid Threats in the Digital Baltic states: A state of the art”, https://www.baltdefcol.org/files/files/publications/Hybrid%20Threats\_LIIA.pdf)LR

In light of power competition vis-à-vis cooperation with the US, NATO, and the EU, and small states standing up to larger powers with nefarious intentions, the drawback is that no entity is capable of defeating all cyberattacks; rather, in order to succeed in cyberspace, the key is learning how to adequately *cope.*24 When it comes to information warfare, and one of the reasons for which it is so dangerous, is that the antagonist need not win – they succeed if they are able to successfully cloud the issue.25 It is no secret that **Russia has waged** **numerous information warfare campaigns in the Baltics** and show no sign of giving up. Recommendations and policy developments Keep on the cusp of cyber hygiene and widely promote amongst citizens: General H.R. McMaster notes the importance of American efforts to conduct reconnaissance in cyberspace and preempt attacks.26 Strive to continuously be one step ahead of hackers. Although this is a daunting, if not (nearly) impossible task, it is one which would involve both governments and the general public. One aspect which has greatly contributed to the success of Estonia in becoming a world leader in cyber defence is investing in people.27 Promoting cyber hygiene is one aspect at which Estonia excels. Raising further awareness about media literacy to combat disinformation and misinformation also helps to win the battle against information warfare. McMaster also advocates for the US to learn from countries which were on the receiving end of Russian aggression.28 As one of the strengths which Estonia possesses is its investment in people, Estonia is a success story in cyber and IT education and training, ranging from kindergarteners to the elderly.29 In an increasingly multipolar world order**, the rise of China presents a serious security challenge** to Europe and the Transatlantic alliance and can be seen on a number of fronts. One of the most pressing, especially when it comes to cybersecurity, is 5G. If seen through the lens of ‘the West’, then a united front should consist of the US and NATO, plus PfP countries, along with the EU in cyber policy. When it comes to 5G, this is especially important. The Baltic states have taken strides to become leaders in 5G policy and can use this opportunity to take a leading role in a Western front in the battlegrounds for 5G policy. Keeping focus on both China and Russia as threats to the security of NATO and the EU: For valid reasons – both historical and contemporary – the Russian Federation is identified as the primary security threat to the 3 Baltic states. The most contemporary events in the neighborhood do not indicate any change in the consistency or persistence of the threat, nor its digital nature. Cyber and hybrid threats directed towards the Baltic states from the Russian Federation will not cease and military, government, and civilian entities need to continue with vigilance, adapt to the rapidly changing nature of cybersecurity and cyberwar, as well as anticipate future changes, staying ahead of the curve. However, despite the very valid concerns over Russian cyber activity, the Baltic states should not neglect such concerns as they relate to China. Indeed, as aforementioned, the Baltic states, especially Lithuania, have taken a firm stance towards China, in cyberspace and beyond, and should continue to use their growing digital prowess to expand their influence in the EU and NATO. Lithuania, under the leadership of Foreign Minister Gabrielius 63 Landsbergis, has increasingly stood up to China.30 Minister Landsbergis’s stance towards China led to him being named as one of Politico’s ‘most influential people in Europe’ – and the only one to make the list from any of the Baltic states.31 Latvia has called upon China to respect the rules of international cyberspace.32 It should be noted that this is certainly not the first time that leaders from the Baltic states have appeared on similar lists, granting small states representation on lists where the usual larger powers within Europe enjoy substantial representation. Such leadership should be emulated, and the digital advances made by the Baltic states provides an ideal way to achieve this, as many countries look to the Baltics as digital leaders. Demonstrating leadership to allies: If ever there was a time, as well as a concrete area for the Baltic states to showcase their strengths as small states, demonstrating leadership in the cyber and tech fields presents the perfect opportunity. Estonia has been the Baltic champion for cybersecurity and e-governance. Lithuania, and to a lesser extent Latvia have shown signs of catching up. Much like offline matters, the three Baltic states use opportunities to meet with US and EU leaders to highlight the dire security situation which the Transatlantic alliance faces from a resurgent Russia – they know from experience and contemporary matters. As the security of cyberspace is one of the acute questions of global politics this century33, cybersecurity and matters of digital warfare will be issues which merit pressing resolve, which is constantly changing. Being on the cutting edge will require countries to remain that way. While member of the United Nations Security Council for the first time, Estonia made cybersecurity a priority, along with the overall security of the region.34 As well, when a member of the UN Security Council, Estonia made it a point to align with the US and the UK to call Russia out over a cyberattack directed at Georgia.35 Latvia and Lithuania have also been active on such fronts. In 2021, Latvia signed an agreement with Poland which establishes a framework for cooperation between Latvia’s Military Information Technology Security 64 Incident Team (MilCERT) and Poland’s National Cyber Security Center.36 Latvia is also taking the opportunity to reach out to the United States to discuss cybersecurity in the region.37 Lithuania has, as aforementioned, developed their own cyber center the RCDC, which is a bilateral LithuanianUS initiative.38 Conclusion To conclude, the domain of cyberspace will be an arena for battle for the foreseeable future. All countries, governments, militaries will be faced with such threats, and the likelihood of businesses and private individuals being faced with such threats is high. The Baltic states are no strangers to such threats and have been leaders in facing up to them. Given the nature of threats faced and the manner in which the Baltics have faced up to them, it is safe to say that the Baltic states will continue to rise up to the challenges and keep up with the rapidly changing nature of cyber threats. However, the last point is the most persisting challenge any entity faces in cyberspace – the need to not only consistently keep up but remain steps ahead of adversaries. The bi- and multilateral agreements made as well as the leadership demonstrated, and the digital awareness can go a long way to not only meet contemporary and future challenges but serve as examples and demonstrate leadership. Cyber and hybrid threats are ominous, but on a positive note, the Baltic states have achieved many remarkable accomplishments in this field.

#### Taiwan-Lithuania cooperation key to defend against Chinese cyberattacks

Cole 21 (J. Michael Cole, Senior Advisor, Countering Foreign Authoritarian Influence (CFAI) at the International Republican Institute (IRI); Global Taiwan Institute, Macdonald-Laurier Institute, Prospect Foundation. Senior Non-Resident Fellow @ Global Taiwan Institute, Masters in War Studies @ Royal Military College of Canada, International Diploma in Humanitarian Assistance @ Fordham University. “The Lithuanian model for expanding Taiwan’s ties with Baltic States”, https://www.caribbeannewsglobal.com/the-lithuanian-model-for-expanding-taiwans-ties-with-baltic-states/)LR

The establishment of a representative office in Lithuania constitutes a victory for Taiwan in its efforts to counter both international isolation and the Chinese narrative of Taiwan’s supposedly inevitable international isolation. By focusing on a part of the world that has not traditionally been an area for Taiwanese presence and engagement, Taipei has also demonstrated the virtues of an asymmetrical approach to combating China on the world stage. This development also exposes the fact that Beijing is willing to break its own rules on “One China,” in that it is now willing to punish states even when they continue to abide by their “One-China Policy” by not establishing official ties with Taiwan. Although the object of Beijing’s ire is ostensibly related to the nomenclature used for Taiwan’s office in Vilnius (which uses the word “Taiwan”), at a deeper level, the source of its anger is the gains that Taiwan has made in Europe, an area where China had hoped to increase its influence. Lithuania has taken some risks in placing its bets on Taiwan, and besides the retaliation it is currently facing, the move may also have cost it future economic opportunities. Consequently, it will be crucial for Taiwan to demonstrate that Vilnius’ risk-taking was not in vain. Already, a large Taiwanese trade and investment delegation has visited the country, with a total of 240 online and offline trade talks involving more than 150 Lithuanian firms and various Taiwanese ones. Taiwan must build on the complementarity of the two economies to replicate its successes in countries like the Czech Republic, where despite much Chinese propaganda, Taiwan has been a much more substantial investor and job creator. Lithuania has a hard-working, highly educated and productive workforce in the manufacturing sector, with strengths in areas such as the laser industry—which has also become a target for Chinese retaliation, with China deciding to halt cooperation between its laser industry bodies and Lithuania. Trade forms the basis of bilateral relations and must be mutually beneficial. Lithuania has made it clear that it expects to reap the benefits of engagement with Taiwan, a country with an economy approximately 11 times larger than its own, as well as a highly advanced tech sector. Lithuania therefore represents a golden opportunity for Taiwan to showcase the advantages of engagement and to demonstrate that small and medium states not only can afford to defy China but can actually benefit materially from doing so. Conversely, failure to build upon and to sustain this momentum could dissuade prospective partners from going down that path. Thus, Taipei must demonstrate a commitment to building prosperous and mutually beneficial ties with its new Baltic ally, and the tangible results must materialize as expeditiously as possible. The potential for engagement between Taiwan and the Baltics goes well beyond trade and investment, however. Lithuania, Latvia, and Estonia all have traditions of resistance to external aggression and, by virtue of their proximity to Russia, have developed their own strategies to counter the security threat posed by their much more powerful – and like China, expansionist neighbor. Taiwan and the Baltic states, therefore, have much to learn from each other, in areas ranging from cyber and hybrid warfare to the implementation of an asymmetrical defense posture. While Russia poses the more immediate threat to the Baltic region underscored by apprehensions across the region that Moscow could launch an invasion of Ukraine as early as next January – it is also clear that China has become a more active player in the region, with all the risks of espionage, cyberattacks, co-optation, and hybrid threats that this new presence entails. Countries like Lithuania that have already defied Beijing are now bracing for the very real possibility of cyberattacks against their institutions, and this is an area where Taiwan’s expertise in addressing such threats can come in handy. **Appropriate intelligence-sharing mechanisms** must therefore be established to facilitate communication, threat mitigation, and response; these are areas where, again, Baltic states can make real gains from a deeper relationship with Taiwan, whose capabilities in the cyber sector are larger by orders of magnitude. The fledgling relationship with this part of Europe also creates opportunities for Taiwan’s indigenous defense industry, particularly in the unmanned vehicle sector: for example, Taiwan donated 10 police drones to Lithuania in October to assist the country as it deals with an influx of refugees from Belarus. For its part, Taiwan has much to learn from the Baltic states in non-traditional military areas, particularly in areas of state resilience and the concept of total defense. For example, as it explores ways by which to increase its deterrence against a Chinese attack, the Taiwanese military could learn important lessons from the Lithuanian Lietuvos Šaulių Sąjunga (“Riflemen’s Union”), the Estonian Defense League, and the National Guard, initiatives that blend traditional military forces with a militia and civilian component. Among other things, Taiwan could learn from those countries’ experiences in providing training to these additional layers of defense, as well as how and where to safely store weapons so that they can be quickly accessed by paramilitary forces in times of national emergency. No doubt Taiwan could learn a thing or two about forming and training a proper Reserve Force. Taiwan and the Baltics can also identify areas for the joint training of special forces and other units charged with waging asymmetrical war against a much more powerful and better-equipped opponent. Latvia and Lithuania, in particular, have clearly signaled their willingness to engage Taiwan more closely on such matters. For this to happen, the Taiwanese government will have to be willing to go beyond its traditional areas of engagement on security issues, and civilian authorities will have to contend with a culture of historical resistance within the ministry of national defense to the idea of giving the population a role in national security (especially one that involves arming them). But as with trade, Taipei will need to overcome those difficulties and, as rapidly as possible, demonstrate to its potential partners that it is ready to engage them in a way that is mutually beneficial. As the experience with Lithuania shows, an unprecedented window of opportunity has been created for Taiwan in the Baltics -one that will not remain open indefinitely. While we cannot expect results overnight, especially on security matters, Taipei cannot afford to drag its feet – and must therefore be proactive in its efforts to turn this potential into a source of real benefits for all the countries involved. It has natural and willing partners in the Baltics; Taipei, too, must demonstrate that it means what it says. If it does well in that area, there is a high likelihood that countries elsewhere will take notice. Failure to seize this moment, however, could have long-term detrimental effects on Taiwan’s appeal, and thereby strengthen China’s ability to deter engagement with Taiwan. The ball, therefore, is very much in Taipei’s court. The main point: A window of opportunity has opened for Taiwan to deepen its engagement with the Baltic states, a grouping of small nations that also faces an existential threat from a powerful authoritarian neighbor. In areas ranging from trade to non-traditional defense, these states are natural allies for Taiwan, and provide a chance for Taipei to showcase the real benefits of closer ties despite threatened retaliation by Beijing.

#### \*\*\*Chinese cyberattacks destabilize Taiwan

* Cyber - -> invasion and PRC can destabilize/counter US forces

Sacks 22 (David, research fellow at the Council on Foreign Relations, where his work focuses on U.S.-China relations, U.S.-Taiwan relations, Chinese foreign policy, cross-Strait relations, and the political thought of Hans Morgenthau. “Enhancing U.S.-Japan Coordination for a Taiwan Conflict”, https://cdn.cfr.org/sites/default/files/report\_pdf/Enhancing%20U.S.-Japan%20Coordination%20for%20a%20Taiwan%20Conflict\_DP\_1.pdf)LR

Adding to the worry, over the past five years China has steadily increased its pressure on Taiwan, reducing the number of mainland tourists who can visit the island, stripping away its few remaining diplomatic partners, placing an embargo on certain Taiwanese exports, ramping up military activities in its vicinity, conducting cyber-attacks, and interfering in Taiwan s democratic process. While Xi continues to publicly stress his commitment to peaceful reunification” with Taiwan and has not introduced an explicit timeline for achieving this objective, he has also said that the Taiwan issue cannot be passed on from generation to generation.”2 He has set 2049 as the date by which China must achieve the great rejuvenation of the Chinese nation,” and achieving reunification” with Taiwan is a core condition for that project.3 Still, it remains unlikely that Xi has already decided to use force against Taiwan, which provides an opening for the United States to adjust its policies and work with its allies to help prevent such an outcome. Although there is debate over whether China will resort to force, China is clearly developing capabilities needed to invade and occupy Taiwan. Preparing for a conflict over Taiwan has driven China s military modernization campaign for the past two and a half decades. China has invested significant resources in developing the tools to defeat Taiwan and prevent the United States from coming to its aid, principally an arsenal of accurate ballistic missiles, the world’s largest navy, hundreds of modern fighter aircraft and bombers, and advanced cyber and counterspace assets The recommendations proposed, while ambitious, are feasible in the current political climate in both Washington and Tokyo, and, with sustained focus in both capitals, can be implemented in the next five years. While China has a number of options it could take to put pressure on Taiwan—seizing an offshore island, initiating massive cyberattacks, firing hundreds of ballistic missiles to take out critical infrastructure, and conducting a quarantine of the island—this paper focuses squarely on how to deter and respond to an invasion of Taiwan. It does so in the belief that Japan s appetite for assisting the United States in countering Chinese aggression against Taiwan short of a full war is politically challenging and likely limited. China is not relying on its inherent advantages, however, and has instead spent the last two and a half decades developing capabilities designed to neutralize U.S. power in the Taiwan Strait. Its military budget has grown from $14.3 billion in 1996 to $252.3 billion in 2020, a nearly eighteenfold increase (see figure 2).7 Preparing for a conflict over Taiwan has consistently driven Beijing s procurement decisions, and China can now bring significant capabilities to bear. The PLA Navy (PLAN) is now the largest navy in the world (as measured by the number of ships, although the United States continues to exceed it by tonnage), with 355 ships and submarines, and is set to grow by nearly 100 ships by the end of the decade.8 The PLA Air Force is the largest air force in the region and is rapidly catching up to Western air forces” and eroding U.S. advantages, according to the U.S. Department of Defense.9 The PLA has one thousand short-range ballistic missiles and six hundred medium-range ballistic missiles in its arsenal.10 China has also established an advanced integrated air defense system on its east coast that can cover Taiwan.11 The PLA is now turning its attention to addressing previous gaps that have persisted, such as anti-submarine warfare, while also rapidly developing information, cyber, and space and counterspace capabilities.12 Taiwan, however, is belatedly recognizing the need to dramatically rethink and invest in its defense. In 2017, its military leadership introduced the Overall Defense Concept(ODC), which aims to develop asymmetric approaches to fend off a Chinese invasion and calls for investing in a large number of smaller, cheaper, and more mobile weapons.23 Rather than seeking to defeat the PLA through attrition, ODC focuses on a decisive fight near Taiwans shores and the prevention of a successful PLA landing. Taiwan has steadily increased its defense budget in recent years, which is now the highest it has ever been in absolute terms.24 More important is using these funds to resource an asymmetric strategy, purchasing missiles, drones, and howitzers.25 There remain obstacles to ODC s implementation, however, and more traditional thinking could well make a comeback.26 All of this means that U.S. intervention on Taiwan s behalf would be a risky and costly proposition, as China can now challenge the United States across all domains and place U.S. aircraft, surface vessels (including aircraft carriers), and bases throughout the Indo-Pacific at risk. In addition, the United States would for the first time be fighting a nuclear-armed opponent with precision standoff weapons, extensive cyberwarfare capabilities, and the ability to target its satellites.27

#### China-Taiwan war goes nuclear. Deterrence is key.

Pettyjohn and Wasser 5-20-2022, \*senior fellow and director of the defense program at the Center for a New American Security, \*\*fellow in the defense program and co-lead of The Gaming Lab at the Center for a New American Security (Stacie and Becca, “A Fight Over Taiwan Could Go Nuclear,” *Foreign Affairs*, <https://www.foreignaffairs.com/articles/china/2022-05-20/fight-over-taiwan-could-go-nuclear/)//BB>

Russia’s invasion of Ukraine has raised the specter of nuclear war, as Russian President Vladimir Putin has placed his nuclear forces at an elevated state of alert and has warned that any effort by outside parties to interfere in the war would result in “consequences you have never seen.” Such saber-rattling has understandably made headlines and drawn notice in Washington. But if China attempted to forcibly invade Taiwan and the United States came to Taipei’s aid, the threat of escalation could outstrip even the current nerve-wracking situation in Europe. A recent war game, conducted by the Center for a New American Security in conjunction with the NBC program “Meet the Press,” demonstrated just how quickly such a conflict could escalate. The game posited a fictional crisis set in 2027, with the aim of examining how the United States and China might act under a certain set of conditions. The game demonstrated that China’s military modernization and expansion of its nuclear arsenal—not to mention the importance Beijing places on unification with Taiwan—mean that, in the real world, a fight between China and the United States could very well go nuclear. Beijing views Taiwan as a breakaway republic. If the Chinese Communist Party decides to invade the island, its leaders may not be able to accept failure without seriously harming the regime’s legitimacy. Thus, the CCP might be willing to take significant risks to ensure that the conflict ends on terms that it finds acceptable. That would mean convincing the United States and its allies that the costs of defending Taiwan are so high that it is not worth contesting the invasion. While China has several ways to achieve that goal, from Beijing’s perspective, using nuclear weapons may be the most effective means to keep the United States out of the conflict. China is several decades into transforming its People’s Liberation Army (PLA) into what the Chinese President Xi Jinping has called a “world-class military” that could defeat any third party that comes to Taiwan’s defense. China’s warfighting strategy, known as “anti-access/area denial,” rests on being able to project conventional military power out several thousand miles in order to prevent the American military, in particular, from effectively countering a Chinese attack on Taiwan. Meanwhile, a growing nuclear arsenal provides Beijing with coercive leverage as well as potentially new warfighting capabilities, which could increase the risks of war and escalation. China has historically possessed only a few hundred ground-based nuclear weapons. But last year, nuclear scholars at the James Martin Center for Nonproliferation Studies and the Federation of American Scientists identified three missile silo fields under construction in the Xinjiang region. The Financial Times reported that China might have carried out tests of hypersonic gliders as a part of an orbital bombardment system that could evade missile defenses and deliver nuclear weapons to targets in the continental United States. The U.S. Department of Defense projects that by 2030, China will have around 1,000 deliverable warheads—more than triple the number it currently possesses. Based on these projections, Chinese leaders may believe that as early as five years from now the PLA will have made enough conventional and nuclear gains that it could fight and win a war to unify with Taiwan. Our recent war game—in which members of Congress, former government officials, and subject matter experts assumed the roles of senior national security decision makers in China and the United States—illustrated that a U.S.-Chinese war could escalate quickly. For one thing, it showed that both countries would face operational incentives to strike military forces on the other’s territory. In the game, such strikes were intended to be calibrated to avoid escalation; both sides tried to walk a fine line by attacking only military targets. But such attacks crossed red lines for both countries, and produced a tit-for-tat cycle of attacks that broadened the scope and intensity of the conflict. For instance, in the simulation, China launched a preemptive attack against key U.S. bases in the Indo-Pacific region. The attacks targeted Guam, in particular, because it is a forward operating base critical to U.S. military operations in Asia, and because since it is a territory, and not a U.S. state, the Chinese team viewed striking it as less escalatory than attacking other possible targets. In response, the United States targeted Chinese military ships in ports and surrounding facilities, but refrained from other attacks on the Chinese mainland. Nevertheless, both sides perceived these strikes as attacks on their home territory, crossing an important threshold. Instead of mirror-imaging their own concerns about attacks on their territory, each side justified the initial blows as military necessities that were limited in nature and would be seen by the other as such. Responses to the initial strikes only escalated things further as the U.S. team responded to China’s moves by hitting targets in mainland China, and the Chinese team responded to Washington’s strikes by attacking sites in Hawaii. A NEW ERA One particularly alarming finding from the war game is that China found it necessary to threaten to go nuclear from the start in order to ward off outside support for Taiwan. This threat was repeated throughout the game, particularly after mainland China had been attacked. At times, efforts to erode Washington’s will so that it would back down from the fight received greater attention by the China team than the invasion of Taiwan itself. But China had difficulty convincing the United States that its nuclear threats were credible. In real life, China’s significant and recent changes to its nuclear posture and readiness may impact other nations’ views, as its nuclear threats may not be viewed as credible given its stated doctrine of no first use, its smaller but burgeoning nuclear arsenal, and lack of experience making nuclear threats. This may push China to preemptively detonate a nuclear weapon to reinforce the credibility of its warning. China might also resort to a demonstration of its nuclear might because of constraints on its long-range conventional strike capabilities. Five years from now, the PLA still will have a very limited ability to launch conventional attacks beyond locations in the “second island chain” in the Pacific; namely, Guam and Palau. Unable to strike the U.S. homeland with conventional weapons, China would struggle to impose costs on the American people. Up until a certain point in the game, the U.S. team felt its larger nuclear arsenal was sufficient to deter escalation and did not fully appreciate the seriousness of China’s threats. As a result, China felt it needed to escalate significantly to send a message that the U.S. homeland could be at risk if Washington did not back down. Despite China’s stated “no-first use” nuclear policy, the war game resulted in Beijing detonating a nuclear weapon off the coast of Hawaii as a demonstration. The attack caused relatively little destruction, as the electromagnetic pulse only damaged the electronics of ships in the immediate vicinity but did not directly impact the U.S. state. The war game ended before the U.S. team could respond, but it is likely that the first use of a nuclear weapon since World War II would have provoked a response. The most likely paths to nuclear escalation in a fight between the United States and China are different from those that were most likely during the Cold War. The Soviet Union and the United States feared a massive, bolt-from-the-blue nuclear attack, which would precipitate a full-scale strategic exchange. In a confrontation over Taiwan, however, Beijing could employ nuclear weapons in a more limited way to signal resolve or to improve its chances of winning on the battlefield. It is unclear how a war would proceed after that kind of limited nuclear use and whether the United States could de-escalate the situation while still achieving its objectives. AN OUNCE OF PREVENTION The clear lesson from the war game is that the United States needs to strengthen its conventional capabilities in the Indo-Pacific to ensure that China never views an invasion of Taiwan as a prudent tactical move. To do so, the United States will need to commit to maintaining its conventional military superiority by expanding its stockpiles of long-range munitions and investing in undersea capabilities. Washington must also be able to conduct offensive operations inside the first and second island chains even while under attack. This will require access to new bases to distribute U.S. forces, enhance their survivability, and ensure that they can effectively defend Taiwan in the face of China’s attacks. Moreover, the United States needs to develop an integrated network of partners willing to contribute to Taiwan’s defense. Allies are an asymmetric advantage: the United States has them, and China does not. The United States should deepen strategic and operational planning with key partners to send a strong signal of resolve to China. As part of these planning efforts, the United States and its allies will need to develop war-winning military strategies that do not cross Chinese red-lines. The game highlighted just how difficult this task may be; what it did not highlight is the complexity of developing military strategies that integrate the strategic objectives and military capacities of multiple nations. Moving forward, military planners in the United States and in Washington’s allies and partners must grapple with the fact that, in a conflict over Taiwan, China would consider all conventional and nuclear options to be on the table. And the United States is running out of time to strengthen deterrence and keep China from believing an invasion of Taiwan could be successful. The biggest risk is that Washington and its friends choose not to seize the moment and act: a year or two from now, it might already be too late.

### 2AC – Israel A/O

#### The plan gets modelled by the middle east. Cybersecurity is key to stop Israel-Iran escalation.

Dana 7-14 [Joseph Dana, 7-14-2022, "Russian Cyberattacks in the Baltics Foreshadow the Future of War", Syndication Bureau, https://syndicationbureau.com/en/russian-cyberattacks-in-the-baltics-foreshadow-the-future-of-war/, DOA: 7-21-2022 //ArchanSen]

In 2014, the country even launched the world’s first e-Residency program with the goal of 10 million e-residents by 2025. Although only 85,000 people have become e-residents so far, the program has allowed entrepreneurs worldwide to set up more than 19,000 digital businesses without needing to be physically present. From freelancers to established entrepreneurs and digital nomads, Estonia’s e-Residency has made it possible to operate an online European Union-registered company from anywhere.

The future of warfare is digital because the future of society is digital. Renewed hostilities between the Baltic states and Russia have become critical laboratories to evaluate where the trend lines of cyber conflict are heading. Countries in the Middle East, such as the United Arab Emirates and Israel, are paying particular attention to how the shifting contours of cyber warfare and defense strategies unfold.

The reason is two-fold. Over the past decade, the UAE has invested substantial resources in following Estonia’s model as a digital republic. From the introduction of blockchain resources on the governmental level to plans to create similar e-residency programs, there is an indelible link connecting the UAE to the Baltics. In recent months, Emirati officials have also discussed the need to build better cyber security infrastructure to safeguard the nation’s knowledge economy.

Many analysts agree that if conflict was to break out between the Gulf states and Iran, it would feature serious cyberattacks from both sides. Israel and Iran have already been trading cyber strikes, and some fear these attacks could escalate beyond military infrastructure and target vital civilian targets.

Whatever happens, cyberattacks will define the future of conflict, and the steps taken by the Baltic states to defend against Russian aggression should be watched closely for clues on how that future will play out.

#### Goes nuclear – US is drawn in.

Dagres 7-13 [Holly Dagres, 7-13-2022, "Biden’s Middle East trip is sending Iran an escalatory message. Here’s why.", Atlantic Council, https://www.atlanticcouncil.org/blogs/menasource/bidens-middle-east-trip-is-sending-iran-an-escalatory-message-heres-why/, DOA: 7-21-2022 //ArchanSen]

US President Joe Biden’s first Middle East trip since taking office comes amid escalating threats of an Israeli military attack against Iran. The visit takes place after talks to revive the Iran nuclear deal ended in Qatar on June 29 without any progress.

“We will not hesitate to use force to keep our citizens safe,” Israeli Prime Minister Yair Lapid said at an Israeli Defense Forces graduation ceremony on July 8. He cited a nuclear Iran, Hezbollah’s precision-guided missiles in Lebanon, and an axis of terror that is trying to entrench itself in Syria as posing challenging threats to Israel’s security.

A former Israeli national security advisor had warned earlier that Israel must prevent Iran from building bases in Syria at any cost. Israel has regularly carried out airstrikes against Iranian-backed forces in Syria—including the bombing of Damascus airport in early June forcing its closure for several weeks—in a bid to stop weapons shipments to Hezbollah, which has close links with Iran. Israel reportedly coordinated these and earlier airstrikes closely with Washington, according to a report published in the Wall Street Journal.

In early June, Israel conducted military drills in the Mediterranean and Red Sea that were clearly meant to send a message that it isn’t ruling out the military option to stop Iran from obtaining a nuclear bomb.

Meanwhile, US patience with Iran is wearing thin; it appears that Biden’s visit to Israel on July 13 and his subsequent meeting with the Gulf Cooperation Council (GCC) and Arab leaders in Saudi Arabia on July 15-16 may likely be a prelude to an escalation against Iran.

# AT: DAs

## Thumpers

#### Baltic wargames thump every disad

McLaughlin 22. Jenna McLaughlin is NPR's cybersecurity correspondent, focusing on the intersection of national security and technology; “Estonia hosts NATO-led cyber war games, with one eye on Russia”; May 2, 2022; NPR; <https://www.npr.org/2022/05/02/1095008257/estonia-nato-cyber-war-games-russia> //BY

TALLINN, Estonia — Two months after Russia's invasion of Ukraine, the cyberwar that experts feared has yet to materialize. But in the tiny Baltic nation of Estonia, digital disaster is playing out nicely.

Over the last week, the NATO Cooperative Cyber Defense Center of Excellence hosted the 10th edition of one of the world's largest annual interactive cybersecurity drills.

Over 2,000 participants from 32 countries formed teams and logged in remotely to help defend regions of Berylia — an imaginary island nation in conflict with its Southern neighbor, Crimsonia — represented by organizers in Tallinn, Estonia's capital city. Participants included cybersecurity experts from governments and private companies, as well as academics.

While the countries are fake, the threats are real — a subject of increasing attention as experts continue to warn Russia could launch destructive digital attacks on Ukraine and its allies in the West.

#### Berylia thumps.

Mclaughlin 22 [Jenna Mclaughlin; NPR's cybersecurity correspondent, Gerald R. Ford Award for Reporting on the National Defense in 2019, finalist nomination in 2020 for the University of Michigan's Livingston Awards; 5-2-2022; "Estonia hosts NATO-led cyber war games, with one eye on Russia"; NPR; https://www.npr.org/2022/05/02/1095008257/estonia-nato-cyber-war-games-russia; KL]

TALLINN, Estonia — Two months after Russia's invasion of Ukraine, the cyberwar that experts feared has yet to materialize. But in the tiny Baltic nation of Estonia, digital disaster is playing out nicely. Over the last week, the NATO Cooperative Cyber Defense Center of Excellence hosted the 10th edition of one of the world's largest annual interactive cybersecurity drills. Over 2,000 participants from 32 countries formed teams and logged in remotely to help defend regions of Berylia — an imaginary island nation in conflict with its Southern neighbor, Crimsonia — represented by organizers in Tallinn, Estonia's capital city. Participants included cybersecurity experts from governments and private companies, as well as academics. While the countries are fake, the threats are real — a subject of increasing attention as experts continue to warn Russia could launch destructive digital attacks on Ukraine and its allies in the West. A scarf with the Ukrainian flag colors is draped over a war hero statue next to the first Estonian armourd car in Tallin, Estonia. Nora Lorek for NPR Estonia's digital revolution In Estonia, where Russia launched one of the earliest destructive cyberattacks in 2007, things are even more serious. After Estonia gained independence from the former Soviet Union in 1991, its leaders pushed for a digital revolution, and today, almost all government and private services are online. During the cyber drills, teams were responsible for protecting those critical services, which were under constant attack. They were tasked with keeping the power grid running, responding to disinformation and propaganda over social media, and protecting a new 5G substation. Lauri Almann, co-Founder of CybExer and former Permanent Secretary of Defense, here at the Cyberex office with view of Old Town of Tallinn. Nora Lorek for NPR Merle Maigre, senior cybersecurity expert at Estonia's E-Governance Academy and former head of NATO CCDCOE. Nora Lorek for NPR They also had to prevent any interference with a financial communication system similar to SWIFT, which allows for secure financial transactions between international banks. Russian banks have recently been banned from SWIFT in light of Russia's invasion. Finally, the exercise included defending remote work environments, an addition inspired by cybersecurity threats emerging from the Covid-19 pandemic. A hotel room as battleground During a tour of the exercise war room at a hotel in Tallinn, organizers from different teams told NPR about the different challenges the teams face. Beyond the technical, that also includes answering legal questions and responding to media requests, making strategic and political decisions, identifying and isolating digital threats as they were launched, and even working with other teams in case of an emergency, like connecting a failing power grid to a neighboring region to keep it online. The name of the exercise, Locked Shields, is inspired by the military concept of linking defenses and working together, explained exercise director Carry Kangur. Locked Shield Excercise at Hilton Tallinn Park. Nora Lorek for NPR Mehis Hakkaja, the founder and CEO of cybersecurity company Clarified Security, was the leader of the red team, or the attackers. He said his team's strategy was to launch distracting, unsophisticated attacks early in the exercise, like website defacements. Then they would slowly burrow their way into a team's office computers and infiltrate the rest of the network. That strategy is a mirror of what happens in the real world. For example, as Russia was launching early cyberattacks during the ongoing war in Ukraine, unsophisticated denial of service attacks on government websites drew attention while Russia was actually launching more destructive and subtle attacks, including deploying wiper malware on satellite servers and other Ukrainian government devices to render them inoperable. Fake targets, real malware The targets in the exercise, like the Berylia Institute of Virology, are fake, but the technology and the malware used to attack it are real. Some of the technology was donated by companies like Siemens, manufacturers of industrial infrastructure. Urmas Ruuto, the Chief of the Technology Branch at the NATO Cyber Center, helped design the game's systems. He showed reporters large screens representing the power grid in Berylia, the water purification system, voice over IP servers representing the phone lines, satellite communications channels, and a financial messaging system. It's easy to track how teams are doing. Siim Marvek, cyber conscript at CR14 Cyber Range. His uniform is made from pixels of photos of Estonian wilderness. Nora Lorek for NPR "If it turns red, that means there is trouble," said Ruuto. And if a team fails to protect its region from an attack on the power grid that would cause physical destruction in real life, the organizers will set off real firecrackers to represent the damage. For the first time this year, teams have to defend a new 5G substation, cutting edge technology that's caused controversy over recent years due to the Chinese company Huawei's ambitions to develop and monopolize its release. Currently, most phone companies claim to have released 5G, but are actually offering 4G with additional bandwidth, Ruuto explained. Additionally, teams faced a wider range of social media influence campaigns. In the war room, organizers in Tallinn had a green screen to film TikTok style videos at any point in the exercise, responding to teams as they posted their own messages. Dr. Adrian Venables, senior researcher at NATO CCDCOE, at the Locked Shield Excercise at Hilton Tallinn Park. Nora Lorek for NPR Estonia's cyber conscripts Siim Marvet is a trainee in Estonia's military Cyber Command unit. His job during the cyber drills was to monitor web logs for potentially suspicious code as well as making sure there was no evidence of website defacements or alterations of digital news articles during the exercise. A patc on Col. Jaak Tarien's uniform. Nora Lorek for NPR Col. Jaak Tarien, head of NATO CCDCOE. Nora Lorek for NPR In Estonia, a small nation on Russia's border, people are still conscripted into military training. Marvet is a cyber conscript, meaning he applied to do his military training with the cyber units, who not only work on computers but are trained in wilderness survival, which includes testing technology in the woods to make sure it would function during a potential conflict. Adrian Venables, the mastermind behind the plot of the cyberwar drill, explained that the scenario focused on disputes between the two imaginary islands and groups of smaller surrounding islands, as well as tensions between minority populations. He told NPR that he had no lack of real-world inspiration when drafting the story teams would engage with. He said he is already working on both the next exercise to take place in Estonia, an offensive cybersecurity drill called Crossed Swords, and next year's Locked Shields. The exercise "has been in the works for a year," explained Col. Jaak Tarien, the director of the NATO Cyber Center, during a briefing. "But the war in Ukraine has been going on since 2014. Russia has been attacking the power grid," for example, he said. Ukrainian businesses were also the target of a destructive attack later called NotPetya, which ultimately got loose and damaged companies around the world, costing billions of dollars in damages. The war unites hackers in the 'free world' The exercise organizers told NPR they were not surprised by Russia's ongoing digital attacks on Ukraine, though Col. Tarien said he was impressed by how Russia's invasion "has united hackers in the free world," referring to how hacktivists from around the world have joined forces with a new Ukrainian volunteer hacker army to target Russia. "It's quite unique," he said. Tarien also said Ukraine has been surprising Russia, both in its military defenses and its ability to fend off cyberattacks. According to Taurien, he still frequently communicates with his colleagues in Ukraine. "When I'm sending emails to them, they are coming back." The text Killnet Hacked You is removed from the outside The NATO Cooperative Cyber Defence Centre of Excellence. Killnet is Russian hacker group. Nora Lorek for NPR Tallinn, Old Town. Nora Lorek for NPR Despite the war, cybersecurity professionals from Ukraine partnered with a team from the United States to participate in the exercise. After some earlier resistance, Ukraine was recently invited to be a contributing member of the NATO Cyber Center, particularly given the valuable intelligence about Russian cyberattacks Ukrainian experts can provide. When the exercise concluded, a Finnish team won, earning the most points in both technical defending and strategic decision making. In Estonia, the target of one of the first major nation-on-nation cyberattacks from Russia, experts and average people alike recognize that digital attacks are a part of Russia's strategy. While cyberattacks haven't been as destructive as many expected in the war on Ukraine, Estonian officials warn that the threat has not been eliminated. "The fact of the matter is that the almighty cyber power of Russia did not roll out," Permanent Secretary Kusti Salm, the highest civilian defense official in Estonia, told NPR. "But clearly it would be extremely false to draw a conclusion that they are not capable."

## A2: Politics

#### The plan is wildly popular – unanimous support for similar legislation.

Grassley 22 [Chuck Grassley, 3-30-2022, "Grassley, Durbin Introduce Legislation to Strengthen Security and Economic Cooperation with the Baltics amid Russian Aggression", No Publication, https://www.grassley.senate.gov/news/news-releases/grassley-durbin-introduce-legislation-to-strengthen-security-and-economic-cooperation-with-the-baltics-amid-russian-aggression, DOA: 7-20-2022 //ArchanSen]

“Not only do I have strong personal ties to the region, but the Baltic countries are essential NATO partners in upholding democratic values abroad,” said Durbin. “Our bill deters Russia from extending Putin’s war into NATO territory, strengthens our partnerships with the Baltics, and enhances their capabilities as critical allies on NATO’s eastern flank. I remain steadfast in my support for the Baltic States as they work to combat Russian aggression as well as Chinese economic pressure.”

More than four million Ukrainians have fled their country since February 24. The Senate unanimously passed a resolution cosponsored by Grassley condemning Russian President Vladimir Putin as a war criminal. In early February – before Putin attacked Ukraine – Grassley and Durbin met with the Lithuanian Delegation to discuss Russian aggression and the impact it would have on the region. Grassley has since led a number of additional efforts to support Ukraine and hold Putin accountable for this unprovoked war.

## USICA

### Aff

#### USICA doomed, Mcconnel is a bitvh – but either way bills aren’t zero sum

Desiderio and Ferris 7-11 ( Andrew Desiderio is a congressional reporter for POLITICO, covering the Senate, national security and foreign policy. He previously covered House investigations and oversight of the Trump administration. He joined POLITICO from The Daily Beast, where he covered Congress with a focus on national security, foreign affairs and Senate campaigns. He previously worked at BBC News and RealClearPolitics. He is a graduate of The George Washington University’s School of Media and Public Affairs, where he studied journalism and Italian language and literature. He hails from Philadelphia and is a proud Philly sports fan. Sarah Ferris covers the House for POLITICO’s Congress team, focusing on the Democratic caucus. She has covered Capitol Hill for six years, including stints focused on budget and health care policy for POLITICO Pro and The Hill newspaper. A graduate of the George Washington University, Ferris spent most of her time writing for The GW Hatchet. She has also written for outlets including The Washington Post, the Houston Chronicle and the Center for Investigative Reporting. “McConnell gets GOP backup in his move to snarl bipartisan U.S.-China bill”, https://www.politico.com/news/2022/07/11/republican-us-china-bill-00045232)LR

McConnell gets GOP backup in his move to snarl bipartisan U.S.-China bill. Senate Republicans are lining up to back Minority Leader Mitch McConnell as he threatens to tank multi-billion-dollar legislation aimed at confronting China, imperiling what initially appeared on track to join this Congress’ biggest bipartisan achievements. McConnell’s threat, sent via tweet while senators were away from Washington, was aimed at derailing Democrats’ fledgling efforts to revive their party-line tax and climate bill, which all Republicans are expected to oppose. Although the Kentucky Republican supported the U.S.-China competition bill, known by some as USICA, he’s now vowing to block it if Democrats move forward with their separate legislation. The move jostled lawmakers from both parties. But even Republicans who toiled on the now-at-risk competitiveness bill are behind him. “USICA is a national security imperative,” said Sen. John Cornyn (R-Texas), whose effort to spur microchip production is included in the legislation. “I interpreted that as Sen. McConnell’s firm indication that he wants us to deal with that and not a partisan reconciliation bill.” Top Democrats say they are unrattled by a McConnell maneuver widely viewed as a last-ditch effort to sink a party-line spending bill that could help them dismantle much of the GOP’s 2017 tax cuts. Moving forward with the tax and climate bill as they brush off McConnell’s posture, Democrats insist the GOP leader has little leverage over their cross-Capitol talks. After three months, negotiators from both parties and both chambers are still finalizing a China competition bill that bridges differences between the House- and Senate-passed versions. The Senate passed its version more than a year ago, with nearly every Democrat and 19 Republicans voting yes. Democrats insist that Republicans who previously backed USICA wouldn’t suddenly oppose it simply because they’re pursuing priorities they’ve gone after since they took power on the Hill. But if their bet goes sour, some Democrats privately acknowledge they have at least one plan B, even if they’re not prepared to use it yet: Ditching cross-aisle bicameral talks altogether and sending the Senate-approved version through the House. On Monday, McConnell argued that a party-line spending bill will “crowd out” the Senate’s ability to pass USICA and “paralyze” the chamber. Cornyn indicated that he wasn’t particularly worried about USICA going by the wayside, citing Democrats’ months-long failure to reach an agreement on their unilateral spending bill — though majority-party senators involved in the talks are hinting at progress in the latest round of talks. Democrats say it shouldn’t be a zero-sum choice between two substantively different bills. They point to McConnell’s own insistence that last year’s bipartisan infrastructure bill proceed separately from an earlier, $1.7 trillion version of this summer’s party-line spending plan. “The right question is how ridiculous is it to kill a bill that you say you like because there’s a different negotiation about a different thing,” Sen. Brian Schatz (D-Hawaii) said. “There’s just no way you can govern that way.” Even before McConnell’s tweet, a growing number of battleground-district House Democrats had been pressuring party leaders to simply take up the Senate version, eager to tout the bipartisan victory back home and anxious that talks could break down fully before November.

## BBB

### Aff

#### Manchin won’t vote, BBB is doomed, Biden has covid

* Can be retagged as a thumper for midterms

Romm and Stein 7-15 (Education: American University, BA in Journalism Tony Romm is the congressional economic policy reporter at The Washington Post, tracking infrastructure reform, government spending and the financial impacts of federal decision-making nationwide. Romm previously covered the tech industry for about 12 years, chronicling the myriad ways that tech companies like Apple, Facebook and Google navigate the corridors of government -- and the regulations that sometimes result. In his time at The Post, where he last served as senior technology policy reporter, he broke many of the most resonant stories on the beat, revealing once-secret information about state and federal probes into Silicon Valley’s largest firms. Romm arrived at The Post in 2018, after previously serving as a senior technology reporter for Politico and a senior editor for policy and politics at Recode, a tech business news site owned by Vox Media. Romm is also an on-air contributor to NBC News and MSNBC. Education: Cornell University, BA in history Jeff Stein is the White House economics reporter for The Washington Post. Since joining The Washington Post in November 2017, he has covered the Republican tax law; the government shutdown; and the administration's economic response to the coronavirus, among other topics. In 2014, he founded the local news nonprofit the Ithaca Voice in Upstate New York. The Ithaca Voice has a full-time staff of reporters and remains the best publication in the city. “Manchin says he won’t support new climate spending or tax hikes on wealthy”, https://www.washingtonpost.com/us-policy/2022/07/14/manchin-climate-tax-bbb/)LR

Sen. Joe Manchin III (D-W.Va.) told Democratic leaders Thursday he would not support an economic package this month that contains new spending on climate change or new tax increases targeting wealthy individuals and corporations, marking a massive setback for party lawmakers who had hoped to advance a central element of their agenda before the midterm elections this fall. The major shift in negotiations — confirmed by two people familiar with the matter who spoke on the condition of anonymity to describe the talks — threatened to upend the delicate process to adopt the party’s signature economic package seven months after Manchin scuttled the original, roughly $2 trillion Build Back Better Act, which President Biden had endorsed. But Manchin told Democratic leaders he is open to provisions that aim to lower prescription drug costs for seniors, the two people said. And the West Virginia moderate expressed support with Senate Majority Leader Charles E. Schumer (D-N.Y.), the party’s chief negotiator, for extending subsidies that could help keep health insurance costs down for millions of Americans, one of the sources said. “Political headlines are of no value to the millions of Americans struggling to afford groceries and gas as inflation soars to 9.1 percent,” said Sam Runyon, a spokeswoman for Manchin. “Senator Manchin believes it’s time for leaders to put political agendas aside, reevaluate and adjust to the economic realities the country faces to avoid taking steps that add fuel to the inflation fire.” The stunning setback late Thursday came despite weeks of seemingly promising negotiations between Schumer and Manchin in pursuit of a broader deal that would have delivered on the promises that secured Democrats control of both chambers of Congress and the White House in 2020. **Without Manchin,** the party cannot proceed in the narrowly divided Senate, since Democrats need all 50 votes in the caucus, plus Vice President Harris’s tiebreaking vote, to use the special process known as budget reconciliation to overcome Republicans’ expected filibuster. Democrats see hope for spending deal with Manchin as Congress returns. To win over Manchin, Democrats already had agreed to surrender their most prized spending proposals, from offering paid family and medical leave to providing child care, free prekindergarten and tax benefits to low-income Americans. But their cuts still proved insufficient for the austerity-minded moderate, who in recent days grew ever more skittish amid reports of record-high prices. This week, new data showed that inflation rose at its highest rate in roughly 40 years, prompting Manchin to tell reporters Wednesday that he would be “cautious” about any new federal spending. But Manchin’s new opposition leaves Democrats in a difficult political bind: They must decide between pressing him after months of false starts or accepting what would still be significant changes to the law lowering health care costs. A package addressing health care, for example, could spare roughly 13 million people from higher insurance costs in January if lawmakers act swiftly. Manchin has endorsed a two-year extension. Similar trade-offs previously prompted Biden’s top aides to deliver a stinging rebuke of Manchin, though the White House late Thursday did not immediately respond to a request for comment.

# AT: CPs

## NATO Key

#### Baltic cyberspace alliance solvency advocate

Libicki 19. Martin C. Libicki is an American scholar and Professor at the Frederick S. Pardee RAND Graduate School in Santa Monica, California; “For a Baltic Cyberspace Alliance?”; 2019 11th International Conference on Cyber Conflict; <https://ccdcoe.org/uploads/2019/06/Art_01_For-a-Baltic-Cyberspace-Alliance.pdf> //BY

* AT: Germany PIC

3. NATO AS A CYBERSPACE ALLIANCE The logic of international alliance is that bigger is usually better when defending against threats.5 Although the size of the alliance and the need for consensus can complicate warfighting,6 the concept of a common defense means that an adversary faces the combined militaries of multiple countries. In a world in which attackers are dissuaded by the prospect that united countries will interpose their forces between attackers and those being defended, the premise that more is better makes intuitive sense. But combat in cyberspace does not really benefit from economies of scale. Within a country, adding more offensive cyber warriors often means lowering the qualifications (at least initially, and perhaps in the long term) for what is, by nature, an inherently elite profession. This means not only that diminishing returns set in, but that the activities of the good-but-not-great can well tip off the other side. So tipped, the other side can improve its defenses in ways that are specific (e.g., vulnerabilities are patched after having been discovered) and general (i.e., a shift occurs in the tradeoff between security and cost/convenience). Correspondingly, the contribution of additional operators is limited. When these operators come from other countries, their contribution is further vitiated unless these countries operate seamlessly. Within an intelligence-sharing alliance (e.g., the Five Eyes), additional members do add heft (each country, for instance, can employ relationships that it has developed with communications companies around the world). Once seams intrude – and these seams are larger within NATO than within the Five Eyes – the level of coordination is less and the prospects for interference (e.g., two countries seeking access to the same target system) are greater. When it comes to defense, the arguments that vitiate the benefits mass are different but similar. A large percentage of all cyber defense efforts requires looking after specific systems. Adding allies adds more systems to defend. This hardly helps defenders of existing systems.7 Although there are defense activities where adding countries may help – e.g., intelligence fusion, collective learning, and forensics – none of these really requires a military alliance, and some of the contributors for these three efforts live in the private realm. Alliances also express their weight through deterrence policies. In the Cold War, the United States deterred attacks by the Soviet Union on NATO allies with a nuclear threat: certainly, if the attacks involved nuclear weapons, and quite possibly if the attack involved overwhelming conventional force. In recent years the U.S. deterrence policy in cyberspace has been notionally extended to a NATO deterrence policy. Unfortunately, U.S. deterrence policy for attacks on the homeland is already an uncertain thing – and extending it adds further uncertainties. There are, for instance, serious questions about what constitutes a cyberattack serious enough to merit retaliation and what the form of retaliation would be; the United States has used sanctions in response to malign cyberspace activities, but there is little evidence that sanctions have deterred Russia, Iran, or North Korea.8 NATO’s retaliation capabilities – which are largely US retaliation capabilities (plus some UK capabilities) – are even less likely to be brought into play if the target of a cyberattack were European. In the five years prior to North Korea’s hack of Sony – which the United States did respond to – South Korea suffered far worse depredations with no U.S. response.9 4. AND WHY IS THE NATO GROUPING NOT THE OBVIOUS ONE? Yet Europeans lean on NATO; in large part, because it already exists and therefore does not need to be invented. But NATO is a military alliance, while cyberspace is essentially a conduit for information,10 hence generally dominated by the community that deals with information qua intelligence. And the existence of the Five Eyes coalition only underlines this point: working relationships among that coalition in the information domain are tighter than they are in the information domain across the NATO alliance. And two of the Five Eyes are not even in NATO. In other words, the real coalition is not doing Europe (the UK excepted) in particular that much good. This matters, because the primary cyber war threat to Europe is from Russia, and the primary targets of Russian coercion are in European countries that face Russia. Two of the countries that face the gravest threats are not even in NATO. Correspondingly, a Baltic cyberspace alliance would have a limited ambit: members would cooperate on defense and aver that a cyberattack on one is an attack on all. In practice, were such an arrangement made, the alliance would have its own definition of what constitutes an “attack”; it might include social media manipulation. A cyberspace alliance, as such, would have three facets but lack one. The first facet is defense: each country would putatively participate more vigorously in those cyber defense activities that benefit from scale, as noted: threat intelligence, forensics, lessons learned. With very large cyberattacks, they could offer mutual aid for systems restoration. The second facet is defense by deterrence. It would require a consensus on what constitutes an actionable offense in cyberspace, notably the type and severity; what responses are appropriate (e.g., to an attack on the local power grid); and what kind of capability is required to retaliate in cyberspace. One rationale for responding in cyberspace is that less forceful options, such as alliance-wide sanctions, are likely to be even weaker than U.S. sanctions are. Conversely, threatening kinetic responses – given the lack of nuclear weapons among proposed alliance members – lacks credibility thanks to Russia’s escalation dominance. The third facet would consist of offensive cyberspace operations used for coercive or, more likely, counter-coercive purposes or for retaliation against grave non-cyber offenses (e.g., the Skripal poisonings11). By contrast, cyberspace operations in support of kinetic operations (e.g., taking a SAM site offline while a NATO sortie flies overhead) would fall outside such an alliance because kinetic operations fall to NATO; if individual members carried out tactical cyberattacks, they would fall under NATO auspices (or their own fights). 5. CHARACTERISTICS AND ADVANTAGES OF A BALTIC CYBERSPACE ALLIANCE What are the characteristics and advantages of such an alliance to its member countries? First, the alliance, limited to cyberspace, would invariably focus on Russia, despite having to tend to other threats (e.g., from China’s commercially-motivated cyberespionage) and despite the possibility that alliance members would probably be diplomatic in public about the alliance’s purpose. Russia’s cyberspace threats are malevolent, politically-directed, and often part of a larger campaign to sow disorder and facilitate coercion. NATO countries, as a whole, are not entirely focused on Russia, these days: those in North America pay as much attention to China;12 those near the Mediterranean tend to look southward. Second, such an alliance would include currently neutral countries, notably Sweden and Finland. Both countries punch above their weight, in cyberspace operations13 and information operations14 respectively. This raises the question: why don’t such countries just enter NATO? To be sure, roughly half the citizens in both countries would like to – but the other half fear, justifiably, a neuralgic Russian reaction if they did (Finland’s accession could put troops along miles of Russian borders). Although Russians would likely react badly to the formation of a Baltic cyberspace alliance, they would have a more difficult time summoning images of jackbooted soldiers while doing so. For Sweden and Finland, the cyberspace alliance could serve as a halfway house. If the Russian threat eases, their entry into NATO can be indefinitely postponed (in the unlikely event that the Russian cyberspace threat disappears, they can leave or the cyberspace alliance might wither away). If the Russian threat persists or worsens, these two countries will have had more practice interoperating with NATO countries, thereby easing their way into an alliance that spans the conventional domains of warfare. Third, a cyberspace alliance would be a mechanism to get Germany to become more involved – or, more to the point, take leadership – in defending Europe against Russia. The current contribution of German military spending (1.2 percent of GDP) to the common defense of NATO is modest. Germany, nevertheless, remains Europe’s largest economy, and would constitute roughly half of the weight of any Baltic cyberspace alliance. Germany has also stepped up smartly in developing its Cyber and Information Domain Service. Its manning, if plans hold,15 would constitute 7.5 percent of Germany’s total force level (13,500 out of 180,000);16 its spending would be 6.3 percent of Germany’s military (41.5 billion Euro) budget.17 By way of contrast, USCYBERCOM’s end-strength goal of 6,000 compares to 1.3 million military personnel in the overall U.S. military – less than a tenth as much concentration on cyberspace. Granted, this is not an apples-to-apples comparison: Germany’s end strength includes electronic warfare battalions; USCYBERCOM’s end-strength does not. But, even after adjustments, Germany’s commitment to fighting in cyberspace, relative to its overall military strength, looks more substantial than the U.S. commitment. Furthermore, a German focus on cyberspace (vis-à-vis kinetic elements of military power) is, again, less likely to engender a neuralgic reaction from Russia (no jackboots, etc.) but does put Russia on notice that its maneuvers in cyberspace have not gone unnoticed and will be resisted by those best placed to resist them. The advantage of such an alliance to its members is that they put the power of all in service of each. This should give Russians second thoughts about their use of cyberspace for offensive purposes – although it may also initially goad them into carrying out operations against the non-NATO countries (Sweden and Finland) to inhibit their participation in such an alliance. Russia’s doing so, conversely, could very well reinforce the value to today’s neutral countries of having others to lean on when facing Russia. The countries in this alliance would be self-selected by virtue of their concern over Russian activities in cyberspace. By contrast, a unified and meaningful NATO response to Russian provocations has to surmount the objections of countries that reserve some sympathy for Russia (Hungary and Greece come to mind). Fourth, this would give NATO competition in the alliance business. Arguably, this would weaken NATO – and is thereby a disadvantage. But competition can also be good: it persuades competitors to listen to their clients (customers, audience, etc.) and induces them to innovate in order to retain their standing. Otherwise, secure in the knowledge that their position is unassailable, they risk becoming sluggish and unresponsive – and when they fall or come apart, it is often “first slowly and then all at once”.18 Thus, when offering cyber security or countering cyberattacks, relevant countries can ask the institutions of NATO and also those of the Baltic cyberspace alliance what each of them can do – each knowing that they are competing both against Russia’s malign influence and the other’s benign influence. But competition can also raise problems: an institutionally aggressive cyberspace alliance may seek greater influence by stretching the definition of a cyberattack: e.g., to include electronic warfare, interference with space operations, and sabotage of or attacks on information infrastructures. 6. ADVANTAGES FOR THE UNITED STATES The most basic advantage is that it makes Europeans more responsible for their own defense, albeit in just this one domain. In the 1980s, for example, three neutral countries – Switzerland, Sweden, and Finland – spent far higher proportions of their income on national defense than most European NATO allies did.19 The “free rider” problem is, if anything, worse today. It may be that much more difficult to persuade European countries to arm themselves if, when such arms have to be used, it would be under a war effort led by the United States. The return of Russia as an aggressive power, since roughly late 2013, may not have been internalized by European countries, concerned as they are with internal fissures – many of which, ironically, were deliberately exacerbated by Russia’s information warfare campaign. And the U.S. pivot to Asia, while more advertised than practiced, would necessarily mean a shift in U.S. resources that would otherwise be available for Europe. But in cyberspace, countries in a Baltic cyberspace alliance would be pooling their resources under either their own individual command (as befits an activity so highly linked to intelligence) or, at least under the command of Europeans. And with the United States not in such an alliance, there is much less of a “free rider” problem (even if Germany would be roughly half the alliance, countries such as Sweden, Finland, and Estonia punch above their weight in this domain). The downside of the upside is akin to the owner of a hammer being persuaded that every problem is a nail: if given a choice between responding to hostile actions in the kinetic world and responding in cyberspace, the latter may be seen as particularly attractive because it relies on tools the alliance can wield themselves rather than tools largely wielded by the United States. Another advantage for the United States is that such an alliance may complicate Russia’s cyber war efforts – largely by increasing the uncertainty that Russian efforts may be met with reprisals: the odds of retaliation from either the United States (as the premier cyberspace power of NATO) or from the Baltic cyberspace alliance will be higher than the odds of retaliation from each of them. This is particularly true for those cyberattacks that leave multiple victims: NotPetya, as an example, levied costs in the hundreds of millions of dollars from Merck and Federal Express (both U.S.-headquartered corporations) and from Maersk (headquartered in Denmark). The raised odds for a response may arise from meeting credibility thresholds (the United States may be wary and the Baltic cyberspace alliance less so or vice versa), attribution thresholds (the United States may have confidence and the Baltic cyberspace alliance may not or vice versa), and damage thresholds (the United States may recognize a higher threshold to warrant its retaliation if the effects of the cyberattack fall primarily on Europeans). Both the United States and the Baltic cyberspace alliance may retaliate but against different targets.20 An associated benefit is that if the modus operandi of whatever cyberspace operations ensue from NATO (that is, in practice, from the United States or the UK) and the Baltic cyberspace alliance are sufficiently similar, it may not be clear to Russia who struck back. This would complicate counter-retaliation targeting (and threats), in anticipation of which retaliation may be more likely, and the prospect thereof more credible. To be fair, attack-retaliation cycles in cyberspace remain loose: the closest example of a retaliatory cyberattack was the late 2012 DDOS campaign against U.S. banks by an Iran that had, two years earlier, discovered that its nuclear program had been set back by the Stuxnet worm. Attack-retaliation-counter-retaliation cycles are even more nthorder relationships. Furthermore, Russia may have the SIGINT or HUMINT to make its own attribution – or it may not care and may conclude that the Baltic cyberspace alliance is an arm of NATO despite the former having neutral countries in it; indeed, it may see all opposing alliances as arms of the United States, facts notwithstanding.

#### NATO is the sole organization that can deter Russia.

Bugajski 16 [Janusz Bugajski, Senior Fellow at The Jamestown Foundation and formerly a Senior Fellow at the Center for European Policy Analysis (CEPA). Bugajski has been a consultant for the U.S. Department of Defense, the U.S. Agency for International Development (USAID), and a course chair for South Central Europe Area Studies at the Foreign Service Institute, U.S. Department of State; 3-29-2016; "Only NATO can defend Europe"; *European View*, Volume 15; https://link.springer.com/article/10.1007/s12290-016-0383-9; KL]

Conclusion

For the US an unstable and insecure Europe that is fractured internally and whose borders are challenged by a belligerent Russia would constitute the greatest foreign policy disaster since the Second World War. To prevent such developments, NATO must revive its core mandate of defending the European homeland and focus less on out-of-area operations. By shifting bases and equipment eastward to confront the newest threats, NATO can help ensure that it has sufficient manpower and firepower to dissuade a Russian offensive against the most exposed Alliance members. An effective NATO remains the key institution for protecting Europe’s security. It may also become the sole multinational organisation that can provide the continent with a measure of policy coherence and maintain the transatlantic link with Washington

#### NATO is key.

Bugajski 16 [Janusz Bugajski, Senior Fellow at The Jamestown Foundation and formerly a Senior Fellow at the Center for European Policy Analysis (CEPA). Bugajski has been a consultant for the U.S. Department of Defense, the U.S. Agency for International Development (USAID), and a course chair for South Central Europe Area Studies at the Foreign Service Institute, U.S. Department of State; 3-29-2016; "Only NATO can defend Europe"; *European View*, Volume 15; https://link.springer.com/article/10.1007/s12290-016-0383-9; KL]

Emerging threats from Moscow

The fourth and most important reason why a substantial NATO military presence in Eastern Europe is vital is that it forms the most effective deterrent and responder to major new threats. Two core challenges emanate from Russia: expansion and implosion. Moscow’s primary objective is to restore Russia as a major pole of power in a multi-polar world. The overarching goal with regard to the West is to reverse US influences in Europe and Eurasia. Russia’s neo-imperial project seeks predominant influence over the foreign and security policies of immediate neighbours so that they will either remain neutral or support Russia’s agenda. In effect, Russia seeks dependent protectorates along its borders, tied into institutions controlled from Moscow (Bugajski and Doran 2016).

While its goals are imperial, the Kremlin’s strategies and tactics are flexible, and this can make them more effective than if they were rigid. Moscow engages in enticements, threats, incentives and pressures, while claiming it is pragmatically pursuing its national interests. It pursues asymmetrical offensives by interjecting itself in its neighbours’ affairs, capturing important sectors of local economies, subverting vulnerable political systems, corrupting national leaders, penetrating key security institutions, challenging territorial integrity and undermining international unity.

Moscow is also not averse to using direct military force, as exemplified by the war against Georgia in August 2008, followed by the forced partitioning of Abkhazia and South Ossetia, and the attack on Ukraine in March 2014 with the annexation of Crimea. According to a recent report by RAND Corporation, given current force deployments, Russia could steamroll across the Baltic states of Estonia, Latvia and Lithuania with ground forces reaching the three capitals in a matter of hours. Without a more intensive regional presence, NATO forces would not have the ability to defend its most exposed states (Shlapak and Johnson 2016). Hence, the factor of deterrence may have limited value if Moscow decides to test NATO’s response.

The RAND report mirrors the concerns of Chairman of the NATO Military Committee General Petr Pavel, who has warned that Moscow could conquer the three Baltic states within two days despite their NATO membership. This is possible because of Russia’s ongoing military expansion, NATO’s relatively slow-moving command structure, and the decline in Alliance capabilities because of lowered defence spending and the withdrawal of US forces, including two heavily armoured US divisions from Germany, with only two now remaining in Europe.

Russia’s potential implosion could present an even more unpredictable future in which NATO would need to manage the multi-regional repercussions. A huge failed state on Europe’s doorstep would have various destabilising consequences for the continent—whether refugee outflows, the spillover of violence, civil wars or the emergence of new aspiring states. Paradoxically, Putin’s attempts to construct a new Russia-centred dominion are likely to accelerate the country’s decline.

An economically and militarily overstretched Russia may witness escalating economic, social, political and sub-regional turmoil and present even more menacing challenges for Western policy. NATO needs to assess the possible consequences of the chaotic downfall of the Putinist system and prepare contingencies for the conflicts that this may generate. In particular, Russia’s neighbours must be shielded from the most destabilising scenarios of civil conflict and Russia’s violent fragmentation, which could spill into NATO territory. By positioning permanent NATO bases in the countries bordering Russia, the Alliance would be better prepared for the negative consequences.

NATO realism

NATO’s European flank remains dependent on the US for its security, as its defence expenditures have been seriously depleted since the end of the Cold War. Without American involvement Europe would be unable to deter an increasingly belligerent Russia. Europe’s demilitarisation over the last decade has coincided with Russia’s military build-up (Michta 2015). The US provides 70 % of all NATO defence spending, while Europe’s contribution to NATO’s military capability is less than 25 %, and the figure is steadily falling. Several countries have decimated their equipment to such an extent that they may be incapable of deploying more than a few thousand troops in the event of outright war. Meanwhile, Russia is re-arming to the tune of $700 billion over the next decade and plans to introduce the next generation of armour, aircraft and missiles, and to modernise its nuclear forces.

## EU CP

### EU CP

#### EU Fails

Libicki 19. Martin C. Libicki is an American scholar and Professor at the Frederick S. Pardee RAND Graduate School in Santa Monica, California; “For a Baltic Cyberspace Alliance?”; 2019 11th International Conference on Cyber Conflict; <https://ccdcoe.org/uploads/2019/06/Art_01_For-a-Baltic-Cyberspace-Alliance.pdf> //BY

One such institution is the EU. Because cyberattacks can influence economic and political well-being, there is a natural compatibility between the EU’s mission and collective action to help promote cybersecurity. Certain critical infrastructures under threat from cyberattack, notably the electric grid, span the EU. Correspondingly, the EU is a vital participant in whole-of-infrastructure protection efforts. But cyber security is not just a matter of hardening networks and systems. It involves intelligence to understand how and why such systems may be attacked and it may 13 involve active defenses to stymie imminent and ongoing cyberattacks.23 There may also be circumstances where reprisals may be called for; even if some reprisals such as economic sanctions can be organized under EU auspices,24 those that involve cyber operations are, again, incompatible with the EU’s purpose. Intelligence, active defenses, and retaliatory cyberattacks are, instead, actions of national security communities. The question of membership in the Baltic cyberspace alliance involves tradeoff: more members means more clout but also less focus and possibly less consensus. As noted, Norway and the Netherlands may be useful members of such an alliance even though neither abuts the Baltic. What about France? On the one hand, France’s emphasis on cyberspace25 looks much like Germany’s, and the bilateral relationship between France and Germany can be understood as the cornerstone of Europe’s stability. On the other hand, geography (e.g., distance from Russia) and history (e.g., former colonies) may lead France to different perspectives from Germany on the Russian threat from cyberspace. What about the UK? On the one hand, the UK government’s skepticism regarding Russian intentions is well understood, and its GCHQ brings considerable assets to the fight in cyberspace. But the UK is part of the Five Eyes group; thus, any intelligence-sharing arrangement the UK has with Baltic states necessary means similar intelligence-sharing arrangements with all the other Five Eyes members (notably, the United States), who may be uncomfortable with such sharing. Furthermore, the advantage of ambiguity afforded by having two independent alliances taking on Russia in cyberspace would be vitiated if both alliances contained the same member

The EU can’t deploy C4ISR, interoperability. It’ll take decades or more.

Meijer and Brooks 21 [Hugo Meijer, CNRS Research Fellow at Sciences Po, Center for International Studies, and the director of the European Initiative for Security Studies; Stephen G. Brooks, a professor of government at Dartmouth College; 4-20-2021; "Illusions of Autonomy: Why Europe Cannot Provide for Its Security If the United States Pulls Back"; MIT Press; https://direct.mit.edu/isec/article/45/4/7/100571/Illusions-of-Autonomy-Why-Europe-Cannot-Provide; KL]

THE COMPLEXITY OF EMPLOYING MODERN WEAPONS SYSTEMS

As dramatic as these weapons shortfalls are, European defense spending—if allocated properly—could eventually secure the needed systems. Yet, not only is the efficient allocation of resources a major challenge because of Europe’s strategic cacophony (as detailed below), but securing the needed weapons systems would only be the first step.

The effective employment of modern weapons systems is far more challenging than in past eras for a variety of reasons. A key consideration is the immense premium put on command, control, communications, computers, intelligence, surveillance, and reconnaissance (C4ISR). C4ISR—often referred to as the “nervous system” of modern militaries—is crucial for gathering information about the combatants, for effectively processing that information, and for disseminating and using that information to develop and implement complex plans.99 NATO’s 2011 mission in Libya shows the heavy reliance of Europeans on the United States’ C4ISR capacity. Europeans would therefore need to develop their own C4ISR capacity to be able to autonomously balance Russia, which would not be an easy undertaking given that Russia is no Libya. They would need large amounts of new C4ISR systems (e.g., reconnaissance and communication satellites; early warning and control aircraft; sensor systems; air, naval, and land command and control platforms), the most complex of which have very long development times. Notably, the already significant difficulty of Europeans assembling the needed systems would be made even more acute if the UK’s exit from the EU ends up meaning that British capabilities also need to be replaced: at present, the UK detains, among other capabilities, 53 percent of the EU’s combat intelligence, surveillance and reconnaissance heavy unmanned aerial vehicles (CISR UAVs), 42 percent of airborne early warning and control aircraft, and 38 percent of electronicintelligence aircraft.100

In addition, European countries lack the kind of specialized personnel needed to operate modern weapons systems effectively. Redressing this weakness would be a significant undertaking, as they have reduced their number of military personnel drastically since the end of the Cold War. As figure 2 shows, the size of the total active militaries of the large European powers declined by 57 percent during the 1990–2020 period.101 Furthermore, beyond the difficulty of securing the financial resources to pay the needed personnel, recruiting sufficient specialized personnel would be a major challenge, as demonstrated by the difficulties faced by many European militaries in attracting personnel for skilled positions.102 Notably, a recent study has shown that the employment of advanced weaponry calls for highly skilled and highly trained military personnel, which are now more difficult to recruit and retain in the military.103 Obtaining specialized military personnel to operate modern weaponry is only the beginning; they must also be trained to effectively use modern weapons, which is extremely challenging and time consuming, partially because these weapons need to be used as part of a cohesive package that places a premium not just on information gathering, but also on coordination and delegation.104 It has taken U.S. military personnel an extraordinarily long time to develop the skills required for effectively using today’s weapons systems: as Posen stresses, the United States’ “development of new weapons and tactics

Chart, bar chart

Description automatically generated

depends on decades of expensively accumulated technological and tactical experience.”105 It would likely take Europeans even longer to develop the needed skills, given differences across countries regarding operational cultures, levels of ambition, languages, and so on.106 Finally, the effective use of modern weaponry in the European theater depends on European forces being able to move quickly and securely over large distances within Europe. Yet, as a UK parliamentary report puts it, “NATO has difficulty moving large forces” across Europe.107 In recent years, the Europeans have sought to bolster military mobility through a variety of initiatives dispersed across different institutions (within both the EU and NATO).108 Yet, the movement and training of military personnel and assets in Europe remain severely hampered by a combination of capability shortfalls, legal/procedural hurdles, and infrastructural deficiencies that will not be easy to resolve.109

#### They can’t build the tech or the vessels.

European defense and technological industrial base = EDTIB

Meijer and Brooks 21 [Hugo Meijer, CNRS Research Fellow at Sciences Po, Center for International Studies, and the director of the European Initiative for Security Studies; Stephen G. Brooks, a professor of government at Dartmouth College; 4-20-2021; "Illusions of Autonomy: Why Europe Cannot Provide for Its Security If the United States Pulls Back"; MIT Press; https://direct.mit.edu/isec/article/45/4/7/100571/Illusions-of-Autonomy-Why-Europe-Cannot-Provide; KL]

THE FRAGMENTATION OF EUROPE’S DEFENSE INDUSTRIAL BASE

If Europeans want to be strategically autonomous, they will have to produce the defense systems they need without being reliant on the United States. The entrenched fragmentation of Europe’ defense industrial base, however, would make this a daunting task.

On the demand side, European states have consistently privileged domestically procured defense equipment over European arms cooperation. According to data from the European Defense Agency, from 2006 to 2015, collaborative defense procurement in Europe accounted for less than one quarter of total procurement.120 For example, a mere 7 percent of the European surface vessels currently in use have been built through European armament cooperation.121 As for fighter aircraft—where the economic incentives for Europeanwide collaboration are especially powerful given the immense cost and complexity of these systems—there has been relatively limited defense cooperation: less than a third (32.6 percent) of combat aircraft used by EU militaries come from European collaborative production.122 Similarly, European states spend more than 80 percent of their military research-and-development budgets within national borders.123

On the supply side, these compartmentalized national markets for weapons systems have resulted in a fragmented and noncompetitive European defense and technological industrial base (EDTIB) characterized by duplication, inefficiencies, endemic overcapacity, and a lack of economies of scale.124 In 2017, 178 different weapons systems were in use in the EU, compared to 30 in the United States.125 As a result, the components that sustain the industrial capacity to deliver high-end to low-end capabilities are scattered across Europe.126 This is a significant problem given that today’s scale requirements are massive for many weapons systems, which also explains why Europe remains highly dependent on the import of key components and weapons systems from the United States.127

Europe has recognized the need for stronger defense production coordination for a long time, and the mechanisms for fostering European-wide collaboration in weapons production have been a topic of discussion for the past several decades. On the demand side, this coordination would require a uniform European procurement policy, with common requirements and with defense industrial cooperation among EU countries being prioritized over national procurement.128 And on the supply side, this would require an integrated defense and technological industrial base (e.g., with one or two major European prime contractors per sector) capable of sustaining military innovation and the development, production, and maintenance of arms at reasonable cost.

Yet, efforts to formulate the kinds of policies that would foster Europeanwide defense collaboration have been feeble. As Matthew Uttley explains, initiatives taken over the years to rationalize and bolster the EDTIB have had a “limited impact,” because governments see a strong national DTIB as a necessary prerequisite for national political sovereignty and, as a result, “national protectionist practices” remain “the dominant driving force in E.U. defense procurement.”129 A report by the European Parliament confirms that a key reason for this lack of collaboration is Europe’s strategic cacophony, specifically, “the current fragmentation of the defense market in terms of demand, regulations, standards and supply.”130

#### The EU doesn’t have unity. The US is key.

Meijer and Brooks 21 [Hugo Meijer, CNRS Research Fellow at Sciences Po, Center for International Studies, and the director of the European Initiative for Security Studies; Stephen G. Brooks, a professor of government at Dartmouth College; 4-20-2021; "Illusions of Autonomy: Why Europe Cannot Provide for Its Security If the United States Pulls Back"; MIT Press; https://direct.mit.edu/isec/article/45/4/7/100571/Illusions-of-Autonomy-Why-Europe-Cannot-Provide; KL]

If the United States were to pull back from Europe, it remains to be seen whether the Europeans could rely on a “Europeanized” NATO, in which the integrated structures would stay in place but without the United States.115 Military planning and C2 require a clear chain of command. When NATO was created, Europeans agreed to be under U.S. military command, rather than attempting the far more difficult task of agreeing to be under the command of another European country or group of European states. More generally, as the hegemonic power in NATO, the United States has facilitated institutionalized cooperation among Europeans and helped partly contain Europe’s strategic cacophony.116 For decades, a U.S.-led NATO has been the overarching shaper of national defense policies and military transformation in Europe, helping overcome coordination and collective-action problems.117 In light of Europe’s deep-seated strategic divisions, a U.S. disengagement would amplify these coordination and collective action problems (assuming NATO survived) and would further hinder institutionalized, intra-European defense cooperation at all levels: strategies and doctrines; training; operational learning; interoperability; and joint capability development. Likewise, without the United States, the persistent and profound divergence of threat perceptions and strategic priorities among Europeans is likely to impede their capacity to agree on shared C2 structures for conducting operations, except for the lowest end of the spectrum of conflict (e.g., peace support operations).118

As a result of strategic cacophony, the EU has, in fact, struggled mightily to create even the most minimal C2 structure. As Luis Simón underscores, “It has taken nearly 20 years of allegedly significant steps for the European Union to establish a ‘Military Planning and Conduct Capability’ composed of up to 25 staffers, devoted to assisting with the planning and conduct of so-called non-executive (i.e., training and assistance) missions,” with an advisory role only.119 Ultimately, given Europe’s deep-seated divergences, there is no basis for optimism that Europeans will be able to agree being under the permanent command of another European country for deterrence and defense or to consistently undertake effective institutionalized military cooperation without the enabling role played by the United States within NATO.

#### Say no. Duplication.

Meijer and Brooks 21 [Hugo Meijer, CNRS Research Fellow at Sciences Po, Center for International Studies, and the director of the European Initiative for Security Studies; Stephen G. Brooks, a professor of government at Dartmouth College; 4-20-2021; "Illusions of Autonomy: Why Europe Cannot Provide for Its Security If the United States Pulls Back"; MIT Press; https://direct.mit.edu/isec/article/45/4/7/100571/Illusions-of-Autonomy-Why-Europe-Cannot-Provide; KL]

THE DIFFICULTY OF INSTITUTIONALIZED MILITARY COOPERATION

An additional challenge is institutional. Europe’s strategic cacophony has prevented Europeans from developing an autonomous, military-planning, command and control (C2) structure.110 Indeed, a report by the European Parliamentary Research Service explains that one of the greatest challenges of European defense is “the lack of integration of the military structures of the Member States.”111 Although an effective and autonomous European defense would require the creation of a permanent planning and C2 infrastructure, the question of developing an autonomous Operational Headquarters (OHQ) has proven highly divisive.112 An OHQ was never established because of conflicting national interests and priorities among Europeans, in particular France, Germany and the UK. Whereas Paris has long supported the establishment of a military OHQ to bolster the EU’s strategic and operational planning structures and its contingency planning and C2 capacity, London has strongly resisted, seeing it as a duplication of NATO’s assets. Germany has stood somewhat in between, though closer to the UK, favoring a focus on civilian-military planning and C2, not least to avoid duplicating structures already existing at NATO.113 As a result, the EU remains entirely dependent on NATO or national assets for the planning and conduct of major executive operations, for which it has no autonomous military structures.114

#### EU involvement causes fights with NATO.

Rzegocki and Ahmed 22 [SaraJane Rzegocki, Program Assistant with the Democratic Resilience Program at the Center for European Policy Analysis (CEPA). She holds an M.A. in Political Science with a concentration in European Union Policy Studies from James Madison University; Alvina Ahmed, Project Assistant with the Atlantic Council’s Transatlantic Security Initiative, part of the Scowcroft Center for Security and Strategy. Previously, she was an intern with the Democratic Resilience Program at the Center for European Policy Analysis (CEPA); 6-27-2022; "No Time for EU-NATO Squabbling as Russian Threat Nears"; CEPA; https://cepa.org/no-time-for-eu-nato-squabbling-as-russian-threat-nears/; KL]

But while unity in condemning the Kremlin’s action among Western nations has been strong, the ability of the EU and NATO to work together to reinforce transatlantic and European security architecture remains in question.

In the late 1990s, the EU’s aspiration to become less dependent on NATO clashed with transatlantic security priorities. Madeleine Albright, then US Secretary of State, warned that European defense must not de-link from NATO, duplicate existing defense efforts or discriminate against non-EU members. Debates over the EU’s strategic autonomy have continued ever since, with member states such as France arguing for greater leadership in European defense, while US administrations complained Europe had been too reliant on American support. Although neither side advocated for European defense completely independent from NATO, debates over greater strategic autonomy and burden sharing have strained transatlantic relations. And despite the US shift of its defense posture to Asia to confront China, administrations have remained dubious over activities outside the Transatlantic alliance.

#### The counterplan destroys readiness, fractures Europe, and triggers war.

Bugajski 16 [Janusz Bugajski, Senior Fellow at The Jamestown Foundation and formerly a Senior Fellow at the Center for European Policy Analysis (CEPA). Bugajski has been a consultant for the U.S. Department of Defense, the U.S. Agency for International Development (USAID), and a course chair for South Central Europe Area Studies at the Foreign Service Institute, U.S. Department of State; 3-29-2016; "Only NATO can defend Europe"; *European View*, Volume 15; https://link.springer.com/article/10.1007/s12290-016-0383-9; KL]

Abstract

Twenty-five years after the end of the Cold War, there is no viable alternative to NATO’s security umbrella over an expanded Europe. The eastern part of the continent is confronting a revisionist and expansionist Russia. Its stability can only be ensured by an effective alliance that establishes permanent bases in the most vulnerable regions as a deterrent to Moscow’s aggression. A strong US presence within a broad alliance that includes all of Europe’s democracies is in America’s national interest and that of all NATO members. This is needed to preserve security across the European continent and to assist in confronting assorted threats to the transatlantic commonwealth.

Introduction

Twenty-five years after the end of the Cold War, there is no viable alternative on the horizon to NATO’s security umbrella over an expanded Europe. The idea floated a quarter of a century ago that Europe could scale down its defences and even dismantle the North Atlantic Alliance exposed a flawed fixation on an ‘end of history’ scenario that has never materialised. In practice, the forces of state nationalism and imperialist revisionism in Russia have proved stronger than those of liberalism and international cooperation with the West.

In many respects, a ‘return of history’ scenario has become more evident in and around Europe, with Russia re-emerging as a revanchist power and threatening Europe’s entire eastern flank. In addition, the EU itself faces existential problems, from the financial and institutional to the demographic and political. In a potentially unstable and fracturing continent, NATO is the sole remaining institution that upholds international security. And it may become the sole multinational organisation that can provide Europe with a measure of coherence. Moreover, NATO is the binding glue of the transatlantic link with Washington.

NATO without alternatives

Several Western European states have hosted US bases since the creation of NATO in April 1949. Since the end of the Cold War and the dismantling of the Soviet bloc in the early 1990s, numerous voices among the new NATO members have called for permanent bases that would include US troops in the eastern part of the continent. Such voices have grown louder as Russia under President Vladimir Putin has become increasingly assertive and is now threatening the independence of numerous states, from the Baltic region to the Black and Caspian Seas.

A NATO alliance that encompasses all of Europe with a permanent multinational military presence in Europe’s east is essential for four fundamental reasons. First, there is no viable alternative to NATO’s political and military structure. The EU does not provide security or generate confidence among states facing potential aggression. The EU’s Common Foreign and Security Policy is primarily a diplomatic mechanism, which openly acknowledges that NATO remains responsible for the territorial defence of Europe. Although the EU has engaged in several peacekeeping, policing and humanitarian missions, NATO possesses the main combat force not only of its European members, but most importantly of the US, which contributes a disproportionate share of Alliance troops, equipment and other resources.

A strong NATO alliance is the backbone of European security. Proposals for a European Army simply dilute and distract attention from the only capable multinational Western security organisation. A European Army would not only siphon off NATO’s already limited assets and diminish its capabilities, but would also trigger rivalries between Europe and North America over the deployment of military forces. Additionally, it could split Europe between countries committed to upholding close security relations with the US and states at a safer distance from Russia that see a lesser need for American security guarantees. Such an outcome would in effect grant Moscow a strategic victory over NATO.

### EU---Britain

#### Britain is key to the Baltics.

Gallardo 22 [Cristina Gallardo, POLITICO reporter; 3-8-2022; "Baltics look to Britain to firm up NATO support"; POLITICO; https://www.politico.eu/article/baltics-uk-security-nato-fears-russia-attack/; KL]

LONDON — Amid fears they could be Russia’s next target, the Baltic countries hope Britain can amplify their calls for more military support from NATO.

Security cooperation between the U.K. and the three Baltic states — Estonia, Latvia and Lithuania — has long been regarded as strong and unaffected by the drama of Brexit.

But since Russia invaded Ukraine last month, this relationship has taken on a new dimension, and become a clear axis in Europe’s wider security debate.

The Baltics have compiled a “wishlist” of demands to better protect their borders, including permanent NATO bases and air defense systems, which the region does not currently have. They are painfully aware that Russian President Vladimir Putin demanded in December that NATO withdraw all its forces from the region, once part of the Soviet Union.

Their requests have met with a sympathetic response in London, where the government is happy to support their case.

Echoing the Baltics’ worst fears, U.K. Defense Secretary Ben Wallace warned last month Putin “will use everything” in the Baltic states. “He doesn’t believe the Baltic states are really countries,” he told the BBC.

A British defense official described the Baltics as “the frontline of NATO security” and said: “We share their concerns that, now more than ever, NATO’s eastern flank needs to deter a Russia that has no regard for international law and sovereign borders.”

In a sign of the importance with which Britain now views the Baltics, the U.K’s Foreign Secretary Liz Truss traveled to the Lithuanian capital Vilnius last week in an attempt to reassure governments it has their back.

“What we have to do now is we have to strengthen NATO, we particularly have to strengthen the eastern flank,” she told the House of Commons Monday. “We have to be serious about defense spending, right across NATO.”

Even with the U.K.’s support, however, the rest of NATO will take some convincing to meet the Baltic demands — and especially to pay for them. For years, NATO hesitated over having significant troop numbers in the Baltic countries amid concerns this could antagonize the Kremlin. Members also worried about the cost of establishing permanent bases in the region and carrying out military exercises.

Baltic wishlist

Edward Lucas, a senior fellow at the Center for European Policy Analysis, said Britain is playing a “very important role” in helping to sort the “mess” that is security in the Baltic region. The current situation, he said, is characterized by “a very complicated command structure, a lack of military clout on the ground, a lot of wishful thinking about how things would sort themselves out in a crisis and a real lack of exercises to tests how things should actually work.”

One reason Britain is well-placed to do this is its leadership of the Joint Expeditionary Force (JEF) of 10 Northern European countries, which includes non-NATO members such as Finland and Sweden as well as Estonia, Latvia and Lithuania.

Launched in 2012, the JEF is seen as more agile than NATO and could provide a rapid response in the first 12 hours should Russia attack one of its members. Rapid deployment of additional troops in the event of an attack is crucial for the Baltics, which are close to signing an agreement among themselves for mobilizing national forces to assist a fellow Baltic country without waiting for a NATO decision, said Rihards Kols, chair of the Latvian parliament’s foreign relations committee.

Through JEF, Northern European countries have already agreed to carry out maritime and air exercises.

“We see the U.K. as very important for our region,” said Kols. “Overall, the U.K. has shown really outstanding leadership in this crisis. We can always say that when it comes to these kinds of situations, the U.K.’s head is on the right place, on the shoulders.”

Gabrielius Landsbergis, Lithuania’s minister for foreign affairs, said the Baltic states are approaching the situation as if they are Western Berlin during the Cold War.

“That means that we need … all the credibility to defend the territory as NATO would defend any other territory in its alliance,” he told a U.K. parliamentary committee last week.

As the most exposed Baltic state, Lithuania has requested a dedicated strategy, Landsbergis said. It fears the Kremlin might attempt to grab the Suwalki gap, a stretch of land connecting Russia’s Kaliningrad exclave on the Baltic Sea with Belarus. British and Lithuanian intelligence forces are now working together to strengthen this area.

Latvia has asked Britain for more maritime and military industrial cooperation, and that aircrafts be placed on Latvia’s military airfields.

Estonia, as the host of a British-led battalion, has seen the number of British troops doubled in recent weeks, and it has received more Challenger 2 tanks and armored fighting vehicles from the U.K.

Long way to go

Although NATO has three such battalions in each of the Baltic countries — with Britain leading the one stationed in Estonia, Canada leading another in Latvia and the U.S. heading the group in Lithuania. These are not intended to withstand a Russian attack but to convey the message to Moscow that any assault would be an attack against the alliance as a whole.

“This relies very much on the idea that Russia wouldn’t want to kill Canadians, Germans or Brits,” Lucas said. “That’s better than nothing and it worked in Western Berlin during the Cold War. But we don’t have air missile defense for those and we need that. And we don’t have the intelligence surveillance and reconnaissance capabilities, and the maritime strategy that we need.”

“Ever since the early 1990s whenever Russia has done something unacceptable we’ve done the minimum to confront it at most or nothing — and then we thought it would go away,” he said. “But every time it comes back.”

Kols said the Baltics were often labelled “alarmists” by EU partners when they flagged concerns about Russia in previous years, adding cooperation with Britain is “paramount.”

Lucas is optimistic that supporting the Baltics is also good for the Brits, particularly since Brexit.

“This gets us back into very close cooperation with European governments,” he said. “Looking at it very crudely, it creates a sort of great pro-British lobby where you’ve got seven countries that are really, really keen and grateful for doing the stuff that we are doing. And that is a good antidote when the French start making fuss about other things.”

#### Exclusion of Britain fails Baltic security.

Simms and Clarke 21 [Brendan Simms, director of the Centre for Geopolitics at Cambridge University; Charles Clarke, Labour politician who served as home secretary from 2004 to 2006; 2-10-2021; "Why Britain matters in Europe"; ; https://www.newstatesman.com/politics/scotland/2021/02/why-britain-matters-europe; KL]

For centuries the United Kingdom has played different roles across Europe, as trading partner, military ally and deadly adversary. Yet nowhere has the relationship been more prolonged and pivotal than in the Baltic Sea. From the heights of medieval trade with the region to its role today as a base for Nato troops, British interests are rooted in Europe’s north-eastern periphery.

The importance of this relationship is unlikely to wane following Britain’s departure from the European Union. The government claims the UK will henceforth pursue a destiny called “Global Britain”. But Britain’s links to the rest of Europe will not only continue to be important, they will become even more so. The EU and the UK are now each other’s most significant neighbour. Britain has a much larger economy than either Russia and Turkey, and offers a potential “soft power” challenge to the EU that Vladimir Putin and Recep Tayyip Erdogan can only dream of.

Most importantly, Europe, and the Baltic especially, depend on the UK for military security. So it is vital that the two great unions understand both each other and the geopolitics of the Baltic Sea and its littoral.

The British-Baltic connection began during the early Middle Ages, when much of northern and eastern England and Scotland endured Viking raids, most of which were launched from Denmark. This is when the phrase “Danegeld” entered the English language, first as a tribute paid to buy off the attackers, then as a tax levied to fund the defence of the realm against them. In the later Middle Ages, many eastern British towns, such as Boston, King’s Lynn, Aberdeen and Edinburgh, were partners of the Hanseatic League, the dominant economic ordering system in the area, which is sometimes compared with the EU today.

Over the next 300 years, relations between England and Scotland (and later Great Britain) and the Baltic became more geopolitical. During the Thirty Years War in the first half of the 17th century, many looked to the Swedish king Gustavus Adolphus to defend the Protestant cause in Germany. During the 18th century, the Baltic became a source of critical naval supplies such as ship masts and hemp. This trade produced its own tensions. In the 1760s, Catherine the Great of Russia wrote in the Nakaz, her Enlightenment-inspired legal manifesto, that Britain was “always exceedingly jealous of the trade carried on with her, and seldom binds herself by treaties with other states, and depends upon no other laws than her own”. This may sound familiar.

Keeping a hostile power out of the Baltic – be it the Catholic League in the Holy Roman empire, Tsarist Russia or France under Napoleon – was central to the British national interest. This involved resisting hostile coalitions such as the first League of Armed Neutrality between 1780 and 1783, an alliance of European naval powers intended to break Britain’s maritime dominance, or the Continental System between 1806 and 1814, which was designed to exclude her from the mainland European economy.

Throughout this period the power of states such as Sweden and Denmark, which had previously played international roles well beyond the region, began to wane. They were caught in the crossfire of the great powers – for example, when Napoleon forced the Swedes and the Danes to take his side against London in the Napoleonic Wars. Wisely, the British did not always react. When, in 1810, Napoleon pressured Sweden into declaring war on Britain, the Royal Navy commander in the region, Admiral Saumarez, ignored the challenge.

During the 19th and early 20th centuries, Britain retained a critical presence in the Baltic. Most of the time, it tried to keep the Russians – Tsarist or Soviet – hemmed in. In 1854, during the Crimean War, the Royal Navy attacked Russian forts off Finland. After the Russian Revolution in 1917, British forces were sent to support the new anti-Bolshevik states – Estonia, Latvia and Lithuania – which emerged from the wreckage. In the first half of the 20th century, the British sought to keep imperial Germany and the Third Reich boxed into the Baltic.

In the course of these operations, Britain became a leading security guarantor of the Baltic states. Estonian independence after 1918 was assisted by the shelter of Royal Navy guns. The Estonian general Johan Laidoner, the commander-in-chief of the country’s armed forces at the time, later reflected that, without the arrival of the British fleet in Tallinn in December 1918, “the fate of our country and our people would have been very different”.

\*\*\*\*

Britain’s relationship with the Baltic has also had its problematic, even traumatic, moments. During the Napoleonic Wars, Britain attacked Denmark twice, both times with dubious legality and to devastating effect. In 1801, the Royal Navy destroyed most of the Danish fleet to prevent it from falling into French hands. Six years later, the British rammed the point home by attacking Denmark’s capital. In the Second World War, the Royal Air Force wrecked Lübeck and Rostock, two of the most beautiful German cities in the Baltic.

There were limits to British power. When London was outraged by the partition of Poland in 1772, British satirists asked whether the navy would sail up the Vistula from Danzig (modern-day Gdansk) to Warsaw in order to bring Russia, Prussia and Austria to heel. Bismarck called Britain’s bluff in 1864 when Palmerston threatened to intervene to support Denmark over Schleswig-Holstein – the north German principality disputed between the German and Danish national movements. If the (then small) British army landed in Germany, Bismarck quipped, he would have it arrested. And having acted as midwife to the Baltic states in 1918-21, the Royal Navy was unable to prevent the Soviet Union annexing them in 1940 and again in 1944.

After the Second World War, Britain remained engaged in the Baltic and, as part of the Nato alliance, was responsible for the defence of the German line there. The objective was to contain the Soviet Union.

But the UK-Baltic relationship gained a new dimension when the UK joined the European Economic Community (EEC) in 1973. Economic relations between Denmark and Britain at that time were so close that the Danes had little choice but to join on the same day. A psychological element was in play, too, because British involvement in the EEC provided a counterweight to what some otherwise regarded as a club of domineering Germans and shifty Latins.

Over the 47 years of Britain’s membership of what became the EU, her relationship with the Baltic developed along diverging axes. On the one hand, as the states of the region integrated with the rest of Europe, the proportion of their trade with Britain declined. On the other hand, the political, geopolitical and demographic connection grew. Britain was strongly committed to steady enlargement of the EU to include the states of the Baltic littoral (Eastern Germany in 1990, Finland and Sweden in 1995 and Poland and the Baltic States in 2004). These countries tended to cleave to the UK in major EU policy debates and on issues such as data protection, human rights and criminal justice.

London used these relationships to try to hedge against Franco-German dominance of the bloc. This was the background to the UK coalition government’s “Northern Future” initiative in 2011.

Furthermore, Britain was militarily the most important of the European Nato nations providing armed deterrence in the region. These links deepened after Putin annexed the Crimea in 2014. Shortly afterwards, things became further complicated by China’s growing presence in the area. The People’s Liberation Army Navy even conducted joint exercises with Russia in the Baltic Sea in 2017. Britain’s defence contribution to the Baltic became even more significant.

Finally, immigration from the region, especially of Poles, Latvians, Lithuanians and Estonians, has been notable since 1945, when many refugees came to work in Britain from those countries. After their accession to the EU in 2004, the number of immigrants from these states grew substantially, and this remains the subject of political controversy.

Then came Brexit. The 2016 referendum was difficult for most Europeans, but it was particularly traumatic for the strongly Anglophile Scandinavians and Balts. There are also worries about security and the strategic ambitions of Putin’s Russia, especially in the eastern Baltic. Is the UK still committed to deterring Russian aggression? Donald Trump’s presidency increased those concerns after he questioned the relevance of Nato’s role in the region.

\*\*\*\*

The UK’s interests in the Baltic today are clear. They are to keep the Russians contained, tensions with Brussels down, EU trade links up, and any future penetration by the People’s Republic of China out. The debate over how to defend these interests formed part of the recent opening of the Baltic Geopolitics Programme at Cambridge University, launched in January this year by the president of Estonia Kersti Kaljulaid and Boris Johnson’s foreign policy adviser John Bew.

Where should the UK now draw the military line in the Baltic? In the past, it has been quite far west, in the Danish Sound, or even in the approaches to the Baltic. It would be far better, though, for Britain to maintain its commitment to defending the democratic countries around the whole Baltic Sea and so to hold the Russians as far east as possible.

This strategy, however, depends on the assumption that the Baltic remains friendly territory. The UK’s post-Brexit relationship with the EU will thus be critical. Britain has no interest in undermining the EU as the principal political and legal ordering system in the Baltic. At the same time, the UK must ensure the region remains an economically shared space. It must not allow the EU’s security pretensions (which, sadly, is all that they are) from disrupting Nato by duplicating and diluting capacity through additional European defence structures.

So far, London has not linked its post-Brexit relationship with the EU to the defence of Europe through Nato by trying, for example, to trade military protection for trade concessions. If tensions arise over fishing or access to the single market, it is to be hoped that Britain will see these as the consequence of Brussels initiatives rather than reflecting some deeper enmity. Even so, it may become difficult to explain to the British public why Britain is militarily defending states dedicated to her economic exclusion, or potentially blocking her access to vaccines developed by British companies with UK government support, but produced on the Continent. The question is particularly pertinent with regard to Denmark, which has taken one of the hardest lines on fishing, citing “historic rights” going back hundreds of years.

Britain is trying to find its new place in the world at a very difficult time. The UK’s relationship to the EU is unsettled and the Covid pandemic poses immense challenges; the economy is in the deepest crisis in modern history and the international situation is in flux, with a new US president, Germany’s election (and Angela Merkel’s succession) in September this year, instability in Russia, and the need for the EU and Nato to regain the trust of domestic and international publics in their effectiveness. This may not seem like the best moment to start talking about Britain’s historical ordering role in Europe.

Soon, though, geopolitics will reassert itself. Britain has mattered and will continue to matter in Europe, especially in the Baltic. The UK shares with the countries of the Baltic Sea region commitments to sustainability, particularly in energy, to the rule of law and human rights, to social stability and cohesion and to excluding political extremism. These common values will matter even more when the substantial increase in defence expenditure authorised by the Johnson administration in 2020 takes effect. In the meantime, the UK should start thinking systematically about its relationship to a vital part of its own continent.

### EU---Canada

#### Canada is key to the Baltics.

Lacroix 16 [Rejeanne Lacroix, research assistant at the Fund for Peace. She holds a Bachelor of Arts in Political Science from Laurentian University in Ontario, Canada and a Master of Arts in International Security Studies from the University of Leicester, United Kingdom. Due to her Slavic maternal heritage, her area of focus is the post-Soviet space and the Balkans where she has contributed widely on de facto states, frozen conflicts, counter-extremism programming and state-building initiatives. Réjeanne has numerous academic publications under her belt ranging from Russian counter-terrorism financing policy, intelligence cultures of Central Asian states, and national security issues. In addition, Réjeanne has a keen interest in compliance and responsible business practices in fragile states and their relation to security.; 12-17-2016; "Guns versus Butter in the Baltics: How Canada Can Help"; NATO Association of Canada Association (NAOC); https://natoassociation.ca/guns-versus-butter-in-the-baltics-how-canada-can-help/; KL]

As Canada prepares to accept a leadership role in NATO operations in Latvia in 2017, it is apparent that Western powers prioritize military strength as the primary method to counter Russian aggression. Modern security threats are a nuanced consolidation of variables. The dichotomy of ‘guns or butter’, or the debate between military force and economic development, is representative of NATO’s mission in the Baltic States. Canadian-led military forces may prevent external Russian incursions but responsibility rests with the individual Baltic States to rectify any concerns from ethnic Russian populations within their borders.

National security concerns over Russian diaspora became prominent once analysts alleged that Russian hybrid warfare techniques would foment separatist sentiments in populations in Russia’s Near Abroad. After the annexation of Crimea and the ongoing conflict in southeastern Ukraine, such circumstances did not seem far-fetched. It is assumed that Russia’s northern neighbours are the next targets of its perceived neo-imperialism due to their relatively small geographic size and substantial ethnic Russian populations. (Estonia 24 %, Latvia 26 %, and Lithuania 6%)

While NATO membership and aid from fellow members in the Alliance alleviates external security concerns in the Baltics, internal difficulties are another matter. Many ethnic Russians are not well assimilated and there are identifiable ethnic grievances. For instance, in Latvia, Russian minorities encounter high rates of unemployment, prejudice, and status as non-citizens. Non-citizens enjoy many of the same rights as Latvian, citizens but they are ineligible to vote and are barred from receiving government pensions. Latvian authorities have attempted to rectify the predicament of non-citizens within its borders by easing language requirements and costs of citizenship testing. Nevertheless, ethnic Russians contend costs remain high, especially for those struggling with unemployment, and thus citizenship remains unattainable. These accusations increase in potency as Latvia continues its struggle with Russian language sources of propaganda.

Estonia exhibits similar inequalities, however the outcome is different. The small Baltic state’s ethnic Russians contend with unemployment and non-citizenship in sizeable numbers, but there is less concern over a consolidation of Russian diaspora. Russian minorities enjoy a sense of security, living side by side with their Estonian neighbours, and a higher standard of living than they would expect in their ethnic homeland. Further, minorities in Estonia have the opportunity to freely contest any of the grievances, such as underemployment or wage disparity, and Estonian media addresses these concerns. In both cases, this is the point where the butter in the ‘guns or butter’ dichotomy takes precedence.

The situation in the Baltics is vastly different from that in Ukraine, and that should be reflected not only in NATO operations, but also in how international partners tackle Russian aggression in the region. Though there are obvious social, economic, and developmental injustices faced by Russian-speaking populations, these problems have not resulted in the organization of Russian diaspora and the promotion of separatist rhetoric. Nevertheless, it is these ethnic grievances that experts anticipate that the Russian Federation will exploit in order to cause political dissent and instability. While a Russian invasion into the Baltics would be an unlikely and imprudent decision, political instability caused by ethnic grievances of considerable minority populations is sufficient to destabilize internal politics. Therefore, it is important for states, such as Estonia and Latvia, to make investments in assimilating their Russian-speaking populations. It is a wise strategy to make efforts to alleviate difficulties faced by Russian ‘compatriots’ living abroad before they become potentially unmanageable political problems. As well, a higher quality of life and integration are prime deterrents against Russian propaganda seeking to discredit Baltic governments.

The Canadian contingent’s foremost responsibilities are to deter any signs of Russian aggression and to ensure that the Baltic States’ sovereignty remains unchallenged. This particular NATO mission will undoubtedly address any concerns regarding external security. On the other hand, the connections fostered between the applicable states and Canadian envoys offers yet another way to safeguard regional security. Canada has valuable experience in developing programs that seek to remedy ethnic grievances faced by various demographics. For instance, shared knowledge could result in ways to make citizenship and language testing more accessible to those non-citizens who wish to pursue that avenue. As well, economic and educational opportunities for the underemployed can be profitable. If welcomed, Canada can be a leader in military affairs and devising socially progressive ways to cement better ethnic relations in the Baltics. If these particular internal issues are addressed, the anxieties over Russia using its expatriates to destabilize Estonia, Latvia and Lithuania lessen considerably.

As Canada prepares to lead a major NATO operation in the Baltics, Estonia, Latvia and Lithuania must consider how they will counter apparent Russian aggression domestically. Security cannot be achieved by relying on military strength alone. It will be a finite balancing act of protecting borders while at the same time charming the hearts and minds of some long time Russian residents; some lacking in citizenship, employment and benefits. In the case where ethnic grievances present the prospect of transforming into a major political issue, social development must enter into national security planning also. Canadian involvement in the Baltics provides yet another occasion for Canadian knowledge to positively influence European security as well as long-term ethnic relations. In the end, security is not a decision of ‘guns or butter’ but rather finding the applicable fusion of both that addresses the specific needs of a region or state.

### EU-NATO CP---Britain

#### UK says no. Trade fights.

Valero 22 [Jorge Valero, Bloomberg reporter; 7-6-2022; "EU’s Sefcovic Signals Possible Trade Retaliation on Brexit Plan"; Bloomberg; https://www.bloomberg.com/news/articles/2022-07-06/uk-plan-on-brexit-seriously-harms-eu-s-interests-sefcovic-says; KL]

The European Union’s chief Brexit negotiator signaled the bloc could impose retaliatory trade measures on the UK over its planned legislation to override parts of the withdrawal agreement, saying the proposal “seriously harmed” the bloc’s interests.

Maros Sefcovic told lawmakers in Strasbourg that if the bill put forward by Boris Johnson’s government is adopted as drafted, “of course in that case we would be forced to use the measures at our disposal, including the measures” in the Trade and Cooperation Agreement, known as the TCA.

The TCA, which was painstakingly hammered out and signed on Dec. 30, 2020 to allow tariff-free commerce, allows for the partial or full suspension of benefits in case of a breach of the Withdrawal Agreement signed between the EU and the UK, including the Northern Ireland protocol. In that case, the EU could slap tariffs on UK exports to its territory.

Sefcovic said that no alternative solution to the Northern Ireland protocol, which keeps the area in the EU’s single market while creating a customs border with the rest of the UK, had been found. “And it is not needed,” he added. He reaffirmed that the EU “wishes to have a positive and stable relationship” with the UK.

The bill put forward by Prime Minister Boris Johnson, which would give Britain the ability to unilaterally amend the post-Brexit settlement for Northern Ireland, risks a trade war with the EU and has soured relations with the UK’s biggest trading partner. The EU relaunched legal action against the UK last month.

“Our interests, as the other party to the agreement, are seriously harmed,” Sefcovic said of the bill.

The EU’s relationship with the UK “must be based on the agreements that both parties negotiated, agreed and ratified: the Withdrawal Agreement and the Trade and Cooperation Agreement,” Sefcovic said.

### EU-NATO CP---Norway

#### Norway says no.

Bjonnes 21 [Roar Bjonnes, co-founder of Systems Change Alliance, long-time environmental activist and a writer on ecology and alternative economics, which he terms eco-economics; 4-23-2021, dated with Wayback Machine; "Why Norway Refused to Join the EU"; Systems Change Alliance; https://systemschangealliance.org/why-norway-refused-to-join-the-eu/; KL]

In 1972, the streets of Norway were filled with protests against the EU when by referendum a majority of Norwegian voters rejected EU membership. The same situation repeated itself in 1994. Throughout the years, opposition against the EU has been dominated by political groups from the centre-left, and especially by farmers, fishermen, and workers on the coasts and in the north. These early protests against the EU reflected, with almost farsighted precision, many of the same topics discussed today in countries like Portugal, Greece and Ireland: lack of democracy, lack of economic justice, lack of freedom and independence, and lack of concerns for the environment.

According to the Norwegian movement against the EU (Neitil EU), which has been active for the past four decades, the main reasons for remaining an independent nation are as follows:

1. Democracy. The authority of ever new areas is transferred from the nation states to the EU. The citizens of the EU are rarely aware of what is happening behind the closed doors of Brussels. Consequently, only around 45 percent of the people of the EU participate in elections. As an independent nation, Norway has a better participatory democracy.
2. Solidarity: As a strong force in the World Trade Organization (WTO), the EU is pressuring poor countries into allowing multinational companies to set up shop. The EU also enters into unfair trade agreements with former colonies and has reduced its aid to poor countries in Africa. The EU pressures poor countries to accept liberalization and privatization of the economy.
3. Environment. The EU is not effectively helping to solve the world’s environmental problems, such as global warming. The EU’s economic policies leads to centralization and large –scale production resulting in overconsumption of resources, increased transport and pollution. The EU has proven to be ineffective in solving global environmental issues and too big and cumbersome to solve local issues.
4. Freedom. After the signing of the Lisbon Treaty much of EU foreign policy decisions are taken during elite political dinners in Brussels and these decisions are increasingly favouring rich countries over the poor. Before membership, Sweden used to vote for the interests of the south in the UN, but as an EU member, Sweden rarely does so. As an outsider, Norway can remain an independent voice in the world.

Two themes have been fundamental to Norwegians against membership in the EU since the Treatise of Rome was signed in 1957: 1) the perception that democratic values at the national as well as the local level are best retained outside the EU, and 2) skepticism towards the market liberalism embedded in the EU constitution. As we have noted above, these concerns have become increasingly prevalent in new member countries, as well, especially those at the periphery of power in Brussels, and in those countries suffering the most from the Euro crisis, such as Portugal and Spain.

According to the ‘No to EU’ movement in Norway, the EU has largely designed a society “where local and national communities are replaced by companies and banks as the fundamental building blocks.” This popular movement has been supported by the majority of Norwegians over the years and has been very critical of the fundamentals in the EU’s economic program, namely the four economic freedoms mentioned above. These neoliberal policies, it is argued, restrict local authorities and states from the right “to limit the market freedoms if it is necessary in order to achieve important social purposes.” In other words, this movement has, from its very inception in the early 1970s, pointed directly to the heart of EUs weak links as an economic and social Union, namely its tendency to centralize and monopolize both economic and political power.

According to the No to EU movement, “The Norwegian Parliament, like Westminster [in Great Britain], is far from the individual voter: Brussels, however, is much farther away and too detached from democratic control. If we want politics based on solidarity values, and if we wish to take the people with us on that endeavour, we must begin at the level where democratic power is real. This is a thesis of equal significance to both Britain and Norway.” Indeed, similar concerns are echoed amongst EU sceptics all over Europe today, from Ireland to Portugal.

### Forward Presence CP

#### Deployments crack unity and cause escalation.

Kühn 18 [Ulrich Kühn, nonresident scholar at the Carnegie Endowment for International Peace, and a senior research associate at the Vienna Center for Disarmament and Non-Proliferation (VCDNP)/James Martin Center for Nonproliferation Studies, based in Vienna, Austria. Previously, he was a Stanton Nuclear Security Fellow with Carnegie’s Nuclear Policy Program, and a fellow with the Institute for Peace Research and Security Policy at the University of Hamburg (IFSH). He holds a PhD (summa cum laude) in political sciences from Hamburg University, an MA in Peace Research and Security Policy from Hamburg University, and a Magister Artium in medieval and newer history as well as German literature from the Rheinische Friedrich Wilhelms University Bonn. His current research focuses on NATO-Russian relations, transatlantic security, nuclear and conventional deterrence and arms control, and the proceedings of the OSCE. Kühn worked for the German Federal Foreign Office and was awarded United Nations Fellow on Disarmament in 2011. He is the founder and a permanent member of the trilateral Deep Cuts Commission and an alumnus of the ZEIT Foundation Ebelin und Gerd Bucerius; 3-28-2018; “NATO’s Options”; *Preventing Escalation in the Baltics: A NATO Playbook*, Carnegie Endowment for International Peace; https://carnegieendowment.org/files/Kuhn\_Baltics\_INT\_final\_WEB.pdf; KL]

If NATO wants to deny Russia the ability to successfully attack one or more Baltic states, it has little choice but to deploy forces on a much larger scale than it currently does. Such forces could be deployed gradually to avoid giving Russia a casus belli and to make such deployments more palatable to skeptical NATO members. The 2017 RAND study proposed deployments of around 35,000 personnel, with an additional reinforcement capability of up to about 70,000 personnel;1 this would certainly prevent a Russian military fait accompli and force Moscow to fight a bloody and drawn-out conventional war, should it attack. These deployments would also, perhaps, eliminate most of the difficulties—and some of the resulting escalation pathways—that stem from the alliance’s current need to reinforce troops rapidly and on a large scale in a crisis. In addition, these troop deployments would raise the costs to Moscow of deliberately forcing a military crisis with NATO.

While such measures might mitigate the short-term risk of deliberate Russian escalation, they would create a number of severe political trade-offs. First, a deterrence-by-denial approach would risk overstretching the delicate political consensus among NATO members about conventional deterrence and assurance. A number of member states, perhaps led by Germany and France, would not support such a policy and would seek to block it. Even more importantly, perhaps, not even the Baltic states are supportive of such a maximalist approach. While many Baltic officials and experts would like to see greater U.S. military engagement in the region, some of them are highly skeptical of the assumptions underlying the RAND war games and think that they are too pessimistic about Baltic defenses. While they would like to see a strong, unified allied response to the growing threat from Russia, they also recognize the need to avoid unnecessarily escalating general tensions with Russia.2 Also, against the background of often contentious debates within NATO about financial and military burden sharing, it would not be clear at all who would provide the necessary funds and forces for such a large military footprint. Neither the United States nor most other allies currently seem to be both willing and capable.

Second, instead of preventing deliberate Russian escalation this deterrence-by-denial approach could, in fact, reinforce Russian perceptions of insecurity. Russia would be loath to accept a NATO force that size so close to its borders. Moscow might seek to prevent NATO force deployments through various means, including, not inconceivably, by considering the preventive use of force (that is, Russia might wage a war because it could only see its position deteriorating in the future). This risk might become more acute in the early stages of a crisis when Russia could misinterpret the large-scale movement of sizable forces, such as the 70,000 personnel reinforcement the RAND study suggested, as NATO preparations for a preemptive attack on Russia. Third, large-scale conventional deployments could help further solidify Russian reliance on its nuclear deterrent and could even serve to lower Russia’s threshold for nuclear use, making the early employment of nuclear weapons more likely.

#### Troops fail. It causes war!

Klein et al. 19 [Colonel Robert M. Klein, Senior Military Fellow in the Center for Strategic Research (CSR), Institute for National Strategic Studies, at the National Defense University; Lieutenant Commander Stefan Lundqvist, Ph.D., Researcher and Faculty Board Member at the Swedish Defence University (SEDU); Colonel Ed Sumangil, USAF, Senior Military Fellow in CSR; Ulrica Pettersson, Ph.D., assigned to SEDU, Adjunct Faculty Member at Joint Special Operations University; 11-2019; "Baltics Left of Bang: The Role of NATO with Partners in Denial-Based Deterrence"; *Strategic Forum* 301, Institute for National Strategic Studies, National Defense University; https://inss.ndu.edu/Portals/68/Documents/stratforum/SF-301.pdf; KL]

As outlined, the RAND scenario leaves NATO with a series of bad options. To deter Russia from such a gambit, the Alliance could deploy ground forces forward in sufficient numbers to defend the Baltics. To this end, the U.S. Army has begun rotating brigade combat teams through the Baltics, and NATO has developed what it calls the Very High Readiness Joint Task Force, a rapid reinforcement capability in the Baltics in the event of a major crisis.4 However, under most likely scenarios, deploying additional conventional ground forces to the Baltics for forward defense is problematic, even if they could arrive in time and in sufficient numbers. First, it remains unclear whether these forces would have the intended deterrent effect. They might instead escalate tensions and stoke Russian aggression because Moscow seems likely to view additional NATO forces in the Baltics as a threat to Kaliningrad and perhaps St. Petersburg. Second, although additional conventional Alliance forces in the Baltics would undoubtedly drive up the costs of conventional attack by Russia, the entire region is one gigantic kill zone where Russia could immediately target NATO forces at the onset of hostilities, including vulnerable assembly areas, supplies, and fuel stocks. Russian attacks emanating through Kaliningrad, from Russia itself, over the sea, and likely from Belarus would almost certainly render additional prepositioned NATO forces vulnerable—at best delaying inevitable Russian victory or at worst dealing the Alliance an overwhelming defeat with very negative political repercussions for NATO.5

#### Forward presence is impossible.

Blachford 20 [Kevin Blachford, Lecturer of International Relations at the Baltic Defence College; 2-7-2020; "Can NATO and The EU Really Defend the Baltic States Against Russia?"; National Interest; https://nationalinterest.org/blog/buzz/can-nato-and-eu-really-defend-baltic-states-against-russia-121711; KL]

Primarily, the challenge facing NATO is dealing with the possibility of Russia using the Baltics as a way to test the credibility of the NATO alliance. The Baltic states of Latvia, Lithuania, and Estonia currently rely on NATO’s enhanced forward presence and air policing missions to deter Russian aggression. But this provides only short term reassurance to the region and overlooks the lessons of the Cold War in which West Germany played a vital role in the credibility of NATO’s deterrence posture. The reluctance of Germany to think seriously about the military security of Europe is, therefore, becoming a hindrance to NATO’s deterrence capabilities. Germany has repeatedly emphasized its aversion to militarism in recent years and its military has faced numerous bouts of austerity. But this reluctance to be seen as a military power overlooks the role of the West German Bundeswehr which acted as the first line of NATO’s defense in the Cold War.

The history of the Cold War provides clues to how deterrence could be increased in the Baltic region today. The defense and deterrence capability of West Germany revolved not just around the nuclear deterrent, but on the ability of the United States and its allies to deploy forces quickly. This related to the logistic capabilities to move forces quickly to the border with East Germany. An important part of NATO strategy therefore relied on the West German autobahns as a way to move both goods and people. Today, the Baltic region lacks any meaningful infrastructure in which reinforcements could be moved quickly to the region. Train lines are outdated and travel between the Baltics to Poland or further to Germany is painstakingly slow. The Baltic states also do not have any significant capabilities to host allied forces in large scale numbers, particularly as access to the area in a conflict scenario would be limited due to Russian air superiority and anti-access, area-denial capabilities. The large placement of U.S. forces in this sensitive area would no doubt invite reprisals and escalation from Russia. But showing the capabilities to quickly respond to a crisis by having the capacity to move resources to the region would enhance NATO’s deterrence in the long term. NATO should therefore consider developing its forces in Germany and even Poland, but with the added caveat of being able to move these forces quickly to where they are needed in the Baltics.

#### Britain and the US say no.

Emmott and Sytas 22 [Robin Emmott and Andrius Sytas, Reuters reporters; 6-15-2022; "The Baltic states want more NATO. They won't get all they seek"; Reuters; https://www.reuters.com/world/europe/baltic-states-want-more-nato-they-wont-get-all-they-seek-2022-06-15/; KL]

Many members, including Britain and the United States, do not favour permanent new bases in the Baltics, three of the diplomats told Reuters. They said it would cost billions and be hard to sustain: The states may not have enough troops and weaponry, and a permanent presence would be highly provocative for Moscow.

"The Baltic states will not each get enough NATO troops to create a division," a NATO diplomat said, referring to their request for up to 15,000 troops across the region, as well as more on stand-by in allied countries to complement national forces. "Whatever is decided must be sustainable."

Instead, allied intelligence will help NATO act if Moscow looks set to invade. During informal discussions at NATO headquarters and in capitals, that view has won over the majority, the diplomats and officials said – the plans will need more work after the summit.

#### NATO says no.

Gallardo 22 [Cristina Gallardo, POLITICO reporter; 3-8-2022; "Baltics look to Britain to firm up NATO support"; POLITICO; https://www.politico.eu/article/baltics-uk-security-nato-fears-russia-attack/; KL]

Even with the U.K.’s support, however, the rest of NATO will take some convincing to meet the Baltic demands — and especially to pay for them. For years, NATO hesitated over having significant troop numbers in the Baltic countries amid concerns this could antagonize the Kremlin. Members also worried about the cost of establishing permanent bases in the region and carrying out military exercises.

## Baltic Army CP

#### Baltic army fails.

Kundla 22 [LTC Tarmo Kundla; Lieutenant Colonel, Commander of the Chair of Tactics. Lecturer, The Estonian Military Academy; 2022; "Strategic leadership requirements for a Baltic unified military effort"; *Ad Securitatem*, Baltic Defence College; https://www.baltdefcol.org/files/files/publications/AdSecuritatem2022.pdf#page=95; KL]

To conclude, there is a need for a strong division-size operationally ready force to defend the Baltic states, but creation of it as a joint Baltic division is probably the biggest strategic leadership challenge that the Baltic states could have. It demands changes in the states’ constitutions, NATO’s framework on its eastern boundary, the Baltic states’ security policy, military build-up, etc. The other option, which is probably more realistic and demands a little fewer change, could be to invest more in the existing NATO framework divisions (MND N and MND NE) regarding capabilities, operational planning, readiness, training, etc., so that those will become fighting forces and not just units on paper. It also means that the Baltic states must take a more active leadership role in those divisions, which is not the case currently.

#### The Baltic division is impossible.

Kundla 22 [LTC Tarmo Kundla; Lieutenant Colonel, Commander of the Chair of Tactics. Lecturer, The Estonian Military Academy; 2022; "Strategic leadership requirements for a Baltic unified military effort"; *Ad Securitatem*, Baltic Defence College; https://www.baltdefcol.org/files/files/publications/AdSecuritatem2022.pdf#page=95; KL]

BALTBAT – why not Baltic Division?

From time to time, people refer to BALTBAT project and ask why the Baltic states have not used it as an example and created a Baltic brigade or even a division. To put it very simply, BALTBAT project cannot be considered as an example for creating a joint force, and forming a Baltic division is much more complicated than it seems.

BALTBAT was founded and designed for peacekeeping missions. The format was chosen not to provoke Russia. Thereby western countries, especially the Nordic countries, were able to equip, train, and develop Baltic militaries in the western way (Ito, 2013 pp. 245-246). The focus solely on peace support operations deviated BALTBAT from the rest of the defence forces and the expertise was not spread among the militaries as intensely as it was desired (Ito, 2013 pp. 254-255). ‘BALTBAT was seen more as a tool for gaining NATO membership and interoperability than as a specific defence capability’ (Grant, et al., 2019 p. 19). Being closed already before 2004, BALTBAT has been activated three more times to contribute NRF. Currently, since 2021, the project has been suspended (Times, 2020).

The Baltic states have never had a desire to have a joint force to defend the Baltic states as a region. The idea of creating the “Baltic state military union” was rejected at the very beginning of the 90s (Molis, 2009 p. 29). The Baltic states became busy to build their own countries and probably were not ready for such level cooperation. In other words, there was lack of strategic thinking and leadership at that time. There is also another and maybe simpler reason for the absence of cooperation: from the distance the Baltic states may look similar, but they are actually very different. ‘History and cultural identity, history of the statehood, language, dominant religion, geographical identification and even major external cultural influences differ considerably in Lithuania, Latvia and Estonia’ (Molis, 2009 p. 29). And lastly, the constitutions of the Baltic states ‘do not permit creating common military forces in the sense of a shared army’ (Miļūna, et al., 2019 p. 63). Therefore, ‘while potential threats from the Russian side and NATO collective defence commitments are similar’ (Andžāns, et al., 2017 pp. 29-30), the Baltic states have developed three different models of militaries (Nikers, et al., 2019). Estonia has followed ‘a compulsory military service and a reservist army, Latvia has opted a solely professional army with a considerably smaller amount of supporting manpower’ (Andžāns, et al., 2017 pp. 29- 30). Lithuania re-established conscription in 2015 and started to use a mixed model relying mainly on professional force, ‘the conscript ratio of the total force structure is and will remain relatively small’ (Jermalavičius, 2017). As independent states, all Baltic countries have followed their own agendas, relied on NATO, and forgot the need for comprehensive regional cooperation when developing their military forces.

## Airpower CP

#### Airpower doesn’t work in the Baltics. Russia invasion would take out airfields first.

BSR = Baltic Sea Region

Klein et al. 19 [Colonel Robert M. Klein, Senior Military Fellow in the Center for Strategic Research (CSR), Institute for National Strategic Studies, at the National Defense University; Lieutenant Commander Stefan Lundqvist, Ph.D., Researcher and Faculty Board Member at the Swedish Defence University (SEDU); Colonel Ed Sumangil, USAF, Senior Military Fellow in CSR; Ulrica Pettersson, Ph.D., assigned to SEDU, Adjunct Faculty Member at Joint Special Operations University; 11-2019; "Baltics Left of Bang: The Role of NATO with Partners in Denial-Based Deterrence"; *Strategic Forum* 301, Institute for National Strategic Studies, National Defense University; https://inss.ndu.edu/Portals/68/Documents/stratforum/SF-301.pdf; KL]

Air Recommendations. NATO can no longer rely on airpower or air presence alone in the BSR to support deterrence by denial or punishment.51 Alliance experts concede that any Russian attack on the Baltic states will likely commence with air strikes against airfields, command and control nodes, and air defense sites of NATO and neighboring non-NATO countries.52 Follow-on attacks from air- and ground-based assets aim to limit Alliance ability to deploy forces forward to counter the Russian offensive. Russian success in such any offensive hinges on surprise and the speed at which its air force can strike targets to slow NATO’s response.53 This situation subverts NATO’s ability to utilize airpower to deter aggression in the BSR and limits the response options available to the Alliance during a crisis.

#### Aircraft fail. Too many deficiencies.

Hendrix 18 [Dr. Jerry Hendrix, formerly a Senior Fellow with the Center for a New American Security (CNAS) and is a retired U.S. naval officer. During his services as a Captain in the U.S. Navy, his staff assignments include tours with the Chief of Naval Operations’ Executive Panel (N00K), the Office of the Undersecretary of Defense for Policy, and the Office of Net Assessment, as well as a stint as the Director of Naval History. Most recently, Hendrix was Director of the Defense Strategies and Assessments Program at CNA; 8-2018; "Filling The Seams In U.S. Long-Range Penetrating Strike"; Center for a New American Security (CNAS); https://s3.us-east-1.amazonaws.com/files.cnas.org/documents/CNASReport-Penetrating-Strike-4.pdf?mtime=20180906151753&focal=none; KL]

Unfortunately, these investments do not go far enough to fill the seams created by deficiencies in previous acquisition decisions. While the department has made a significant investment in fifth-generation stealth strike fighter aircraft, none of them have sufficient range to reach their targets without the assistance of large “big wing” tankers, which are susceptible to attack from enemy A2/AD systems, a critical vulnerability.10 Attempts to pair these aircraft with long-range missiles with sufficient range to reach deep into A2/AD “bubbles” to reach critical strategic targets are hampered both by slow development of modern weapons to replace Tomahawk cruise missiles based on 1970s-era designs and by a lack of capacity within the defense industrial base and the logistics supply chain to keep forward shooters well supplied during high-tempo combat operations.11 Additionally, there are command and control difficulties associated with missile control after launch in competitive spectrum and cyber environments.12

Perhaps most concerning to planners is that the U.S. Navy’s carrier aviation arm, composed of 11 supercarriers and 10 accompanying air wings of approximately 60 aircraft, is not optimized to execute long-range penetrating strike missions. The carriers, given their size and electronic emissions, are vulnerable to attack by antiship ballistic and cruise missiles and hence are restricted to operating in excess of 1,000 nautical miles (nm) from enemy shore.13 Air wing aircraft, largely consisting of F/A-18 C/D/E/F Hornets and F-35C Lightning II aircraft, which have unrefueled ranges of 500nm and 630nm respectively, are unable to reach enemy targets without tanking.14 As mentioned previously, large Air Force “big wing” tankers are too vulnerable to penetrate A2/AD bubbles, and the Navy currently lacks sufficient organic mission tanking to effectively extend the range of the air wing.15 Oddly, naval aviation has consistently either fumbled or bypassed opportunities to develop new longrange strike aircraft that could maintain the relevance of the carrier itself in future security environments dominated by A2/AD technologies.16

## Unilat CP

#### Unilat fails.

Urbelis 20 [Vaidotas Urbelis, Defence Advisor at the Lithuanian Embassy in the U.S., former Defence Policy Director at the Ministry of National Defence of the Republic of Lithuania, lecturer at General Jonas Žemaitis Military Academy of Lithuania and the Institute of International Relations and Political Science of Vilnius University; 2020; "The New United States defence strategy: consequences for the Baltic states"; *Lithuania in the Global Context: National Security and Defence Policy Dilemmas*, Chapter 4, General Jonas Žemaitis Military Academy of Lithuania; https://kmilc.lka.lt/data/Leidiniai/sisteminis\_katalogas/Socialiniai\_mokslai/Politologija/2020-Cesnakas-Lithuania%20in%20the%20global%20context.pdf#page=65; KL]

In the U.S. strategy, the defence of Lithuania, like other Baltic states, is based on the viability of the NATO organization and its ability to defend its members. Theoretically, the U.S. could provide bilateral security guarantees to Poland or the Baltic states, but because of the geographical location, their defence requires the involvement of the Allies. German, Belgian and Dutch ports and railways, Norwegian and British fleets and French rapid response forces can be best utilized under NATO’s framework. Therefore, the U.S. looks to the defence of the Baltic states primarily through NATO and coordinates its plans accordingly.

## AT: EU-NATO CP

#### NATO says no---internal politics

Zandee et al. 21. Dick Zandee is Senior Research Fellow and Head of the Security Unit of the Research department of the Clingendael Institute. Prior to his work at Clingendael, he was Head of the Planning & Policy Unit of the European Defence Agency; “Countering hybrid threats”; October 2021; Clingindael Institute; <https://www.clingendael.org/pub/2021/countering-hybrid-threats/> //BY

Since the beginning of EU-NATO cooperation, there have been obstacles that have hindered the optimalisation of cooperation, leading to sub-optimal outcomes. Some obstacles are age-old, others have emerged over time as a result of the changing security environment.

The first and most important obstacle to further cooperation is the organisations’ difference in member states. Although there is quite some overlap – 21 states are both a member of the EU and NATO – there are also EU countries that are not a NATO member and vice versa. The differences in membership are especially an obstacle when it comes to sharing more sensitive security-related information. It is common that some states only want to share information with either the EU or NATO, but not with both. Bruno Lété of the German Marshall Fund of the United States describes this as follows: “(…) the EU and NATO nevertheless remain two separate bodies, and each uphold restrictive information-sharing procedures that prevent the emergence of a culture of shared situational awareness or cyber threat assessment.”﻿[[75]](https://www.clingendael.org/pub/2021/countering-hybrid-threats/3-eu-nato-cooperation-what-has-been-achieved-so-far/)

In practice, this problem is sometimes solved through sharing information only between EU and NATO staff, explicitly mentioning that information cannot be shared with representatives from member states. In such situations, NATO and EU staff are able to cooperate on the basis of this information, while at the same time individual member states do not receive the classified information. This way of information sharing has enabled the EU and NATO to circumvent certain (political) obstacles.﻿[[76]](https://www.clingendael.org/pub/2021/countering-hybrid-threats/3-eu-nato-cooperation-what-has-been-achieved-so-far/) So far, this construction has worked for EU and NATO staff, but if joint EU-NATO follow-up action would be required, the involvement of member states cannot be avoided and political obstacles would then still prevail. Moreover, the absence of a secure communication system sometimes also makes this very difficult. Even if there is a willingness among EU and NATO staff to share sensitive or classified information, there is no quick and easy communication system to share this information. Moreover, the EU’s and NATO’s standards and practices in securing information also diverge﻿[[77]](https://www.clingendael.org/pub/2021/countering-hybrid-threats/3-eu-nato-cooperation-what-has-been-achieved-so-far/), which further complicate matters. Therefore, this possibility of circumventing the (political) obstacles is no sustainable solution for the long term.

## EU---Canada

#### Canada is key to the Baltics.

Lacroix 16 [Rejeanne Lacroix, research assistant at the Fund for Peace. She holds a Bachelor of Arts in Political Science from Laurentian University in Ontario, Canada and a Master of Arts in International Security Studies from the University of Leicester, United Kingdom. Due to her Slavic maternal heritage, her area of focus is the post-Soviet space and the Balkans where she has contributed widely on de facto states, frozen conflicts, counter-extremism programming and state-building initiatives. Réjeanne has numerous academic publications under her belt ranging from Russian counter-terrorism financing policy, intelligence cultures of Central Asian states, and national security issues. In addition, Réjeanne has a keen interest in compliance and responsible business practices in fragile states and their relation to security.; 12-17-2016; "Guns versus Butter in the Baltics: How Canada Can Help"; NATO Association of Canada Association (NAOC); https://natoassociation.ca/guns-versus-butter-in-the-baltics-how-canada-can-help/; KL]

As Canada prepares to accept a leadership role in NATO operations in Latvia in 2017, it is apparent that Western powers prioritize military strength as the primary method to counter Russian aggression. Modern security threats are a nuanced consolidation of variables. The dichotomy of ‘guns or butter’, or the debate between military force and economic development, is representative of NATO’s mission in the Baltic States. Canadian-led military forces may prevent external Russian incursions but responsibility rests with the individual Baltic States to rectify any concerns from ethnic Russian populations within their borders.

National security concerns over Russian diaspora became prominent once analysts alleged that Russian hybrid warfare techniques would foment separatist sentiments in populations in Russia’s Near Abroad. After the annexation of Crimea and the ongoing conflict in southeastern Ukraine, such circumstances did not seem far-fetched. It is assumed that Russia’s northern neighbours are the next targets of its perceived neo-imperialism due to their relatively small geographic size and substantial ethnic Russian populations. (Estonia 24 %, Latvia 26 %, and Lithuania 6%)

While NATO membership and aid from fellow members in the Alliance alleviates external security concerns in the Baltics, internal difficulties are another matter. Many ethnic Russians are not well assimilated and there are identifiable ethnic grievances. For instance, in Latvia, Russian minorities encounter high rates of unemployment, prejudice, and status as non-citizens. Non-citizens enjoy many of the same rights as Latvian, citizens but they are ineligible to vote and are barred from receiving government pensions. Latvian authorities have attempted to rectify the predicament of non-citizens within its borders by easing language requirements and costs of citizenship testing. Nevertheless, ethnic Russians contend costs remain high, especially for those struggling with unemployment, and thus citizenship remains unattainable. These accusations increase in potency as Latvia continues its struggle with Russian language sources of propaganda.

Estonia exhibits similar inequalities, however the outcome is different. The small Baltic state’s ethnic Russians contend with unemployment and non-citizenship in sizeable numbers, but there is less concern over a consolidation of Russian diaspora. Russian minorities enjoy a sense of security, living side by side with their Estonian neighbours, and a higher standard of living than they would expect in their ethnic homeland. Further, minorities in Estonia have the opportunity to freely contest any of the grievances, such as underemployment or wage disparity, and Estonian media addresses these concerns. In both cases, this is the point where the butter in the ‘guns or butter’ dichotomy takes precedence.

The situation in the Baltics is vastly different from that in Ukraine, and that should be reflected not only in NATO operations, but also in how international partners tackle Russian aggression in the region. Though there are obvious social, economic, and developmental injustices faced by Russian-speaking populations, these problems have not resulted in the organization of Russian diaspora and the promotion of separatist rhetoric. Nevertheless, it is these ethnic grievances that experts anticipate that the Russian Federation will exploit in order to cause political dissent and instability. While a Russian invasion into the Baltics would be an unlikely and imprudent decision, political instability caused by ethnic grievances of considerable minority populations is sufficient to destabilize internal politics. Therefore, it is important for states, such as Estonia and Latvia, to make investments in assimilating their Russian-speaking populations. It is a wise strategy to make efforts to alleviate difficulties faced by Russian ‘compatriots’ living abroad before they become potentially unmanageable political problems. As well, a higher quality of life and integration are prime deterrents against Russian propaganda seeking to discredit Baltic governments.

The Canadian contingent’s foremost responsibilities are to deter any signs of Russian aggression and to ensure that the Baltic States’ sovereignty remains unchallenged. This particular NATO mission will undoubtedly address any concerns regarding external security. On the other hand, the connections fostered between the applicable states and Canadian envoys offers yet another way to safeguard regional security. Canada has valuable experience in developing programs that seek to remedy ethnic grievances faced by various demographics. For instance, shared knowledge could result in ways to make citizenship and language testing more accessible to those non-citizens who wish to pursue that avenue. As well, economic and educational opportunities for the underemployed can be profitable. If welcomed, Canada can be a leader in military affairs and devising socially progressive ways to cement better ethnic relations in the Baltics. If these particular internal issues are addressed, the anxieties over Russia using its expatriates to destabilize Estonia, Latvia and Lithuania lessen considerably.

As Canada prepares to lead a major NATO operation in the Baltics, Estonia, Latvia and Lithuania must consider how they will counter apparent Russian aggression domestically. Security cannot be achieved by relying on military strength alone. It will be a finite balancing act of protecting borders while at the same time charming the hearts and minds of some long time Russian residents; some lacking in citizenship, employment and benefits. In the case where ethnic grievances present the prospect of transforming into a major political issue, social development must enter into national security planning also. Canadian involvement in the Baltics provides yet another occasion for Canadian knowledge to positively influence European security as well as long-term ethnic relations. In the end, security is not a decision of ‘guns or butter’ but rather finding the applicable fusion of both that addresses the specific needs of a region or state.

## EU-NATO CP---Britain

#### UK says no. Trade fights.

Valero 22 [Jorge Valero, Bloomberg reporter; 7-6-2022; "EU’s Sefcovic Signals Possible Trade Retaliation on Brexit Plan"; Bloomberg; https://www.bloomberg.com/news/articles/2022-07-06/uk-plan-on-brexit-seriously-harms-eu-s-interests-sefcovic-says; KL]

The European Union’s chief Brexit negotiator signaled the bloc could impose retaliatory trade measures on the UK over its planned legislation to override parts of the withdrawal agreement, saying the proposal “seriously harmed” the bloc’s interests.

Maros Sefcovic told lawmakers in Strasbourg that if the bill put forward by Boris Johnson’s government is adopted as drafted, “of course in that case we would be forced to use the measures at our disposal, including the measures” in the Trade and Cooperation Agreement, known as the TCA.

The TCA, which was painstakingly hammered out and signed on Dec. 30, 2020 to allow tariff-free commerce, allows for the partial or full suspension of benefits in case of a breach of the Withdrawal Agreement signed between the EU and the UK, including the Northern Ireland protocol. In that case, the EU could slap tariffs on UK exports to its territory.

Sefcovic said that no alternative solution to the Northern Ireland protocol, which keeps the area in the EU’s single market while creating a customs border with the rest of the UK, had been found. “And it is not needed,” he added. He reaffirmed that the EU “wishes to have a positive and stable relationship” with the UK.

The bill put forward by Prime Minister Boris Johnson, which would give Britain the ability to unilaterally amend the post-Brexit settlement for Northern Ireland, risks a trade war with the EU and has soured relations with the UK’s biggest trading partner. The EU relaunched legal action against the UK last month.

“Our interests, as the other party to the agreement, are seriously harmed,” Sefcovic said of the bill.

The EU’s relationship with the UK “must be based on the agreements that both parties negotiated, agreed and ratified: the Withdrawal Agreement and the Trade and Cooperation Agreement,” Sefcovic said.

## Delay CP

### Delay CP

This may already be a case with different highlighting

#### Now is key.

Tol et al. 22 [Jan van Tol, Senior Fellow at the Center for Strategic and Budgetary Assessments. Prior to his retirement from the Navy in 2007, Captain van Tol served as special advisor in the Office of the Vice President. He was a military assistant to Andrew W. Marshall, the Secretary of Defense’s Principal Advisor for Net Assessment, from 1993–1996 and 2001–2003. At sea, he commanded three warships, two of which, USS O’Brien (DD-975) and USS Essex (LHD-2), were part of the U.S. Navy’s Forward Deployed Naval Forces based in Japan. Captain van Tol’s analytic work has focused mainly on long-range strategic planning, naval warfare, military innovation, and wargaming. He holds a B.A. in Philosophy and Logic from the University of Massachusetts/Amherst and a M.S. in Operations Research from the Naval Postgraduate School, and graduated with distinction from the College of Naval Command and Staff at the U.S. Naval War College; Christopher Bassler, Senior Fellow at the Center for Strategic and Budgetary Assessments, where he researches technology & innovation, joint aerospace capabilities, maritime operating concepts, and overall U.S. & allied military strategies. He served as a civilian in the Department of Defense, for both the Departments of the Navy and the Air Force, as an engineer, designer, strategist, and advisor. His previous assignments include the F-35 Joint Program Office, the Office of the Chief of Naval Operations (OPNAV) in the Pentagon, the Office of Naval Research, and the Naval Surface Warfare Center, Carderock Division. He has worked in various capacities to enhance capabilities and interoperability across all warfighting domains, in many technology areas, and with key allies and partners on five continents, including NATO for both the capabilities and the S&T Organisation. He was awarded two U.S. Patents. Dr. Bassler received two U.S. Navy Meritorious Civilian Service Awards, from the U.S. Secretary of the Navy and the Chief of Naval Research. His degrees include a Ph.D. in Aerospace Engineering from Virginia Tech; a M.A. in Security Policy Studies from the George Washington University Elliott School of International Affairs; and a Diploma in Strategy & Innovation from the University of Oxford, Saïd Business School; Katherine Kjellström Elgin, Fellow at the Center for Strategic and Budgetary Assessments. She brings rigorous research to policy discussions and has held positions in both academic and policy organizations. Prior to joining CSBA, she served as a DAAD Post-Doctoral Fellow at the Foreign Policy Institute of Johns Hopkins School of Advanced International Studies (SAIS), where she wrote and published on grand strategy, great power relations, U.S. defense strategy, European security, and alliance management. Dr. Elgin has also worked at the Brookings Institution and with the Long Term Strategy Group in Washington, D.C. In 2018, she served as a visiting fellow at the Institute for Security & Development Policy in Stockholm, Sweden. Dr. Elgin earned her Ph.D. in Public Affairs (Security Studies) from Princeton University’s School of Public & International Affairs. At Princeton, she served as the director of the Center for International Security Studies’ Strategic Education Initiative, leading the university’s program for educating and mentoring students with an interest in national and international security; Tyler Hacker, Analyst at the Center for Strategic and Budgetary Assessments. His work focuses on U.S. defense strategy, future warfare, and great power competition. Prior to joining CSBA, Tyler was an analyst at the Congressional Research Service, where he conducted research on topics in defense logistics. Tyler previously served as a field artillery officer in the United States Army in Germany, where he participated in NATO operations and exercises in Poland, Romania, and the Baltic states. He has also completed internships at the U.S. Army War College and the American Enterprise Institute. He holds a B.A. in International Studies from Virginia Military Institute and an M.A. in Security Studies from Georgetown University; 2022; "Executive Summary"; *Deterrence and Defense in the Baltic Region: New Realities*, Center for Strategic and Budgetary Assessments (CSBA); https://csbaonline.org/uploads/documents/CSBA8312\_(Deterrence\_Defense\_Baltic)\_web.pdf; LR + KL]

The NATO posture “reset” announced by Secretary Stoltenberg, if properly and promptly executed, could greatly reduce the potential for a Russian fait accompli against the Baltic states as well as deter aggression against other NATO states on the eastern border. Presently it is broadly supported among the NATO member states because of the ongoing Russia-Ukraine war and its accompanying atrocities. However, depending on the evolution of the conflict, the enthusiasm and willingness of some member states may flag over time or individual member state priorities may start to shift. For any reset to be successful, there must be genuine burden-sharing among all member states, whether on the eastern front or not, until NATO’s “reset” is fully implemented.

## Nukes CP

#### Any posture change erodes unity.

Kühn 18 [Ulrich Kühn, nonresident scholar at the Carnegie Endowment for International Peace, and a senior research associate at the Vienna Center for Disarmament and Non-Proliferation (VCDNP)/James Martin Center for Nonproliferation Studies, based in Vienna, Austria. Previously, he was a Stanton Nuclear Security Fellow with Carnegie’s Nuclear Policy Program, and a fellow with the Institute for Peace Research and Security Policy at the University of Hamburg (IFSH). He holds a PhD (summa cum laude) in political sciences from Hamburg University, an MA in Peace Research and Security Policy from Hamburg University, and a Magister Artium in medieval and newer history as well as German literature from the Rheinische Friedrich Wilhelms University Bonn. His current research focuses on NATO-Russian relations, transatlantic security, nuclear and conventional deterrence and arms control, and the proceedings of the OSCE. Kühn worked for the German Federal Foreign Office and was awarded United Nations Fellow on Disarmament in 2011. He is the founder and a permanent member of the trilateral Deep Cuts Commission and an alumnus of the ZEIT Foundation Ebelin und Gerd Bucerius; 3-28-2018; “Preventing Escalation in the Baltics: Introduction”; *Preventing Escalation in the Baltics: A NATO Playbook*, pages 7-11, Carnegie Endowment for International Peace; https://carnegieendowment.org/files/Kuhn\_Baltics\_INT\_final\_WEB.pdf; KL]

All these developments create political (as well as military) problems for NATO. They lead to pressure on NATO to review its own deterrence and defense posture, including its nuclear component, and, perhaps, to formulate more muscular responses. But such a debate—already tentatively taking place at NATO Headquarters—risks eroding unity among NATO allies, which have a wide range of different preferences in the nuclear realm. This erosion of unity could undermine deterrence. A military alliance at odds over its own deterrence and defense posture could be perceived as weak by Russia, making it a potential target for military blackmail and coercion.

## Hotlines CP

#### Hotlines encourage risky behavior.

Faure 22 [Juliette Faure, PhD candidate in political science at Sciences Po Paris; 3-17-2022; "The US-Russia military hotline in Europe: Key principles for risk reduction from the US-Russia deconfliction measures in Syria"; European Leadership Network; https://www.europeanleadershipnetwork.org/commentary/the-us-russia-military-hotline-in-europe-key-principles-for-risk-reduction-from-the-us-russia-deconfliction-measures-in-syria/; KL]

The increasing reliance of the US and Russia on military deconfliction channels to sort out confrontational relations between them, however, should be seen as buying time for diplomatic tracks to manage and eventually solve the conflict. Whilst military hotlines are essential to avoid misunderstanding and escalation precipitating a conflict between two nuclear-armed military powers, they also might change the incentives for aggressive and risky behaviour in the international arena if they are perceived to be reducing the need for diplomatic dialogue and genuine risk reduction measures.

#### Russia says no. Ukraine proves.

Bertrand 22 [Natasha Bertrand, CNN reporter; 3-16-2022; “NATO has tried to reach Russia unsuccessfully via deconfliction hotline”; CNN; <https://edition.cnn.com/europe/live-news/ukraine-russia-putin-news-03-16-22/h_221942ac8c75ff9e244b6001e7cdff3a>; KL]

NATO has tried unsuccessfully to connect with Russia via a deconfliction hotline and written letters as Russia’s invasion of Ukraine has spread further west toward NATO territory, senior NATO military officials said on Wednesday.

“We are trying to communicate with them of course,” one of the officials told reporters in a briefing at NATO headquarters. “But it requires two [sides] to communicate.”

The US also has a separate deconfliction hotline with Russia that it has tested and has determined is functioning but has not yet used in practice, officials have said.

The officials’ comments followed Russia’s attacks on a Ukrainian military base earlier this week just 10 miles from the Polish border, which raised concerns about the conflict potentially spilling over into a NATO member country.

amongst EU sceptics all over Europe today, from Ireland to Portugal.

## Norway PIC

#### Norway is key. Incorporation reassures Russia and provides experience to allies, especially the Baltics.

Marius Kristiansen 7-12-2022. MS in Defense Analysis, Non-Resident Fellow with the Irregular Warfare Initiative, officer in the Norwegian Special Operations Command. Njål Home, Norwegian Special Operations Command. "Small state security sector assistance in the age of great power competition". Comparative Strategy an International Journal. https://doi.org/10.1080/01495933.2022.2087435. Pen-DL

Geopolitical realities, being NATO’s front to the northeast, largely defines Norwegians strategic- and security policy. The Russian bear is our neighbor and represents the strongest permanent military presence in our part of the High North. This is unlikely to change overnight, and Russia will thus remain “the defining factor of Norwegian defense planning in the foreseeable future.”5 Russia is also occupying a gradually more prominent place on the competitive stage, challenging western dominance and allied coherency. So amidst the (re-)emergence of great power competition, Norway is also predicated to take a greater responsibility for deterrence prior to aggression. Not necessarily because the relationship with Russia is set to deteriorate, but due to “growing uncertainty surrounding allied support to Norway in the most likely crisis scenarios.”6

Preserving regional (and global) stability is paramount for Norway’s security. Historically, Norway’s relations with Russia have consisted of a delicate balance of deterrence through NATO membership and reassurance through self-imposed military and nuclear restraints, diplomacy, and cooperation whenever possible. Reassurance might be described as a Norwegian strategic niche. Before the Baltic countries became members of NATO, Norway was the only NATO country that bordered Russia. General Philip Breedlove (former Supreme Allied Commander Europe [SACEUR]) describes Norway’s strategic role this way: “In NATO, we see Norway’s leadership in the way it handles relations with Russia. Norway has a long history of working with Russia in the border areas. You have experiences that we can learn from in NATO.”7

However, given the immense military asymmetry between Norway and Russia, Norway is not able to generate any (significant) regional deterrent effect on its own. Thus, Norway is dependent on NATO regional and global deterrence capability to credibly succeed in deterring Russia. The reliance on NATO still complicates the value of deterrence – in the same manner as deterring a bully through having an older cousin that knows karate has it apparent limitations. The old, and friendly, relationship between the two neighbors is thus not only convenient, but a necessary and complementary security and stability tool. For NATO this also has obvious value; a more bellicose ally on the northeastern frontier could certainly create some predicaments for the alliance. As it stands, Norway offers a stable and predictable partner for both parties – thereby extending the value of reassurance to the relationship between Russia and NATO as a whole.

Norway’s contribution of reassurance is valuable, but that can hardly be seen as a sufficient contribution in an alliance. At least from a realist perspective, such soft power contributions are not far from “free riding.” The reliance on “deterrence by proxy” requires commitments and investments in a more profound way. Norway contributes with niche reassurance capability, is just above the NATO 2% GDP target,8 and has shown will and ability to work closely with allied strategic resources to demonstrate its deterrence capability.9 While these (and more) are important lines of operations, Norway must also seek to maintain and offer relevant capabilities to fulfill international expectations in other alliance-endeavors. In support of global peace and security NATO must have “the military capacity to undertake crisis management operations alone,10” and this requires active participation – also from small states. In a time where alliance cohesion is being challenged, military and security “protectionism” is counterproductive. An overly inwards focus to the detriment of supporting other campaigns may both undermine national political capital and the alliance itself. Norwegian politicians and flag-officers will do well to keep in mind that the performance of the alliance along the entire conflict spectrum is essential both for cohesion and the perception of deterrence that can be generated. “Ultimately, NATO’s strength and value lies in the unity and interoperability of its members.”11

Deterrence through proxy – Investing correctly in a strong alliance

In one way or another Norway has a long history of investing in security, both close and “out-of-area.” Early Norwegian international military engagements after World War II focused mainly on reconstruction in Europe. In parallel, Norway engaged itself in UN (and otherwise)-led peace operations, from United Nations Emergency Force (UNEF) in 1956 until present day. When the global war on terror kicked off, Norway refocused its effort and initiated two decades of Norwegian alliance- and coalition-engagements abroad. Through its engagements, Norway has sought to be both an altruistic team-player on the world stage and a loyal alliance member. With the (re-)emergence of great power competition, these efforts have taken a back seat in the security discourse – presenting Norway and its allies a di- and occasionally tri-lemma.

Analysis suggests that in the midst of a new and more competitive normal, rather than merely refocusing at home – shutting the windows and locking the door – the relevance of using military means abroad in a globalized world will only increase. Beadle and Diesen suggest this is valid regardless of changes in the threat at home. 12 The interconnectedness of all actors makes it difficult to isolate both the problem and the solution geographically. The dilemma is that, although one acknowledges the need for allied solidarity in coping with global threats to secure a vital and effective alliance, there is also a strong urge to strengthen national defense. If you add the increasing military costs, you might end up as Norway has tended to – reducing size and refocusing on national defense.13 This might be well in line with the core task of collective defense in NATO’s Strategic Concept, but to the detriment of the remaining two core tasks of crisis management and cooperative security.14

## Türkiye PIC

#### Exclusion wrecks cohesion and cyber defense. Estonia stans Türkiye.

Daily Sabah 22 [Daily Sabah with AA; 1-20-2022; "Turkey is good NATO ally with high capabilities: Estonian FM"; https://www.dailysabah.com/politics/diplomacy/turkey-is-good-nato-ally-with-high-capabilities-estonian-fm; KL

Estonia sees Turkey as a good NATO ally with high capabilities, which understands its security concerns very well, the country's Foreign Minister Eva-Maria Liimets said Friday.

Speaking to Anadolu Agency (AA) during her official visit to Turkey, Liimets said that the bilateral relations between the two countries are evolving every year and said: "Estonia and Turkey are two very good allies in NATO."

Noting that the relations between Turkey and Estonia date back a century, Liimets said, "We will celebrate the 100th anniversary of our diplomatic relations in 2024. All this time, we have had very good relations between our countries that have developed and strengthened with each passing year."

Expressing that the two countries focused on bilateral relations, economy and security, Liimets added that Estonia is planning to diversify its ties and look into different sectors. "Tourism is one of the important areas. I am very happy that we also have direct flights between Istanbul and Tallinn, the capital of Estonia. So there is a lot to talk about and much to progress."

Liimets stated that there will be more parliamentary interaction between the two countries this year and that business delegations will visit each other and said that trade, digital and defense cooperation between Turkey and Estonia will progress.

On the two countries' cooperation in the field of security and their NATO partnership, she said: "Estonia and Turkey are two very good allies in NATO. We see Turkey as a very capable, good ally who understands our security concerns very well. Therefore, we think there are opportunities for closer cooperation. We are grateful for Turkey's commitment to NATO."

Reminding that a few years ago, Turkish pilots undertook the task of protecting the Baltic airspace within NATO, Liimets said that they are grateful to Turkey for its contribution to this security issue, which is important for Estonia and the Baltic countries.

Regarding the planned visit of the Estonian Chief of General Staff Martin Herem to Turkey, Liimets said, "It is very nice that our chiefs of staff can come together and discuss these issues, since we cooperate very closely in NATO."

Drawing attention to the issue of cyber security, Minister Liimets stated that Turkey is a member of the NATO Joint Cyber ​​Defense Center of Excellence in Tallinn and that the two countries are also cooperating closely in this field.

Migrant issue

Another point that Liimets touched upon was the migration crisis. Stating that Turkey's geographical location is at the crossroads of the migration crisis, Liimets said: "We really appreciate Turkey's approach to the issue, which hosts millions of refugees on its territory."

Underlining that Estonia has been providing financial aid to migrant camps in Turkey and other countries, she said: "We see that millions of Syrians are forced to leave their country. We must all try to do our best so that this country can find a political solution and all refugees can safely return to their homeland."

#### Turkey’s still on the edge. Cooperation tips them to our side, which wins the Ukraine war.

Rogin 22 [Josh Rogin; Washington Post columnist; 6-30-2022; "How a thaw with Turkey could help Ukraine win the war"; Washington Post; https://www.washingtonpost.com/opinions/2022/06/30/biden-erdogan-thaw-turkey-help-ukraine-against-russia/; KL]

At this week’s NATO summit, President Biden met for the first time in a year with President Recep Tayyip Erdogan, setting aside his long-standing issues with the Turkish leader. But Turkey continues to play both sides of the Russia-Ukraine conflict. If the United States is now willing to deal with Ankara, the next deal should center on persuading Erdogan to side with the West on Ukraine.

There’s no love lost between Biden and Erdogan. As a senator, Biden was a regular critic of Turkey, owing in part to the strong Greek American constituency in his home state of Delaware. As vice president, Biden clashed with Erdogan over the Turkish leader’s backsliding on democracy and human rights. But despite their mutual dislike, Erdogan has long sought Biden’s validation. This week’s phone call and bilateral meeting in Madrid with the U.S. president allowed Erdogan to project himself to his people as an important leader on the world stage.

The White House insists there was no quid pro quo. Yet officials privately acknowledge that the close timing of the Biden administration’s newfound enthusiasm about selling F-16 fighter planes to Turkey and Erdogan’s decision to allow NATO to move forward with membership for Sweden and Finland is no coincidence. This shows that the U.S. side is realistic about the transactional nature of the relationship. Erdogan has always been — and probably always will be — a problematic ally who demands concessions for doing the right thing.

This week’s positive Biden-Erdogan interactions offer the chance for a significant upgrade of relations after years of mutual neglect and distrust. If both sides can muster the political will to keep going, the next step would be to bring Turkey on board with regard to the Ukraine crisis.

There are many ways Turkey could be more supportive of Ukraine — if the United States and the West can convince Erdogan that this is in his interest. Turkey not only has refused to join sanctions on Russia but also has become a key place for sanctions evaders. That has to stop. A Turkish firm linked to Erdogan’s family is giving Ukraine advanced drones, which is good, but for months, Ukraine has sought more Turkish arms to include things such as anti-missile systems, missiles and electronic warfare capabilities.

Turkey could have the biggest impact by helping break the Russian naval blockade of Odessa. By preventing grain exports, the Russians are tanking the Ukrainian economy and fueling a global food crisis.

“The Biden administration’s apparent support for new F-16s for Turkey may be just the beginning of a strategy to bring Ankara along and incentivize the Turkish government to move away from diplomacy with Russia in favor of participating in an international effort to secure Ukrainian agricultural exports,” Steven Cook, a senior fellow at the Council on Foreign Relations, told me.

Erdogan announced last week that his government will begin talks with Moscow about opening “corridors” for grain exports, but that’s likely just a stall tactic by the Russians. When the futility of that effort plays out, Turkey will have to decide whether to join Ukraine’s partners to facilitate the exports without Russia’s permission.

“Cracking open those ports may require a more direct role for the United States and NATO,” Cook said. “Turkey would be important in that effort as a Black Sea power and the country that controls the Bosporus Strait.”

To be sure, expectations that Erdogan will fully break with his friend, Russian President Vladimir Putin, should be set low. The Turkish leader, who faces political headwinds at home in advance of an election next year, also has an incentive to continue mobilizing his nationalist followers by demonizing the United States via his state-controlled media.

But Biden’s national security adviser, Jake Sullivan, has long argued for a more transactional approach in the U.S.-Turkey bilateral relationship. Sullivan laid out this argument in a 2018 commentary he co-wrote with Eric Edelman, a former U.S. ambassador to Turkey.

“You’ll never have a full rapprochement with Turkey,” Edelman told me. “What you will have is a series of one-off deals. And that’s not necessarily bad.”

There are good reasons to think Erdogan’s long flirtation with Putin is no longer paying him dividends. Turkey must no longer see Russia as a reliable arms supplier. The war in Ukraine is helping push inflation in Turkey to unprecedented levels, devastating its already shaky economy. Turkey has also been confronting Russian forces in several places, including Syria, Libya and Nagorno-Karabakh.

Sure, the United States could wait to see whether Erdogan falls from power. But there is no guarantee that whatever government comes next would be a better security partner in Ukraine. Erdogan is the problematic ally we know — and right now, he looks to be in a mood to make deals.

The Biden administration would be better off holding its nose and moving forward on improving relations with Turkey, rather than spending its limited diplomatic time and energy focusing on partners that have less ability or will to help, such as Saudi Arabia. Bringing Ankara on board could be the key to helping Ukraine break the stalemate and win the war.

#### Turkish-NATO relations contain Russia. The relationship is sustainable but on the brink.

Kara 22 [Mehtap Kara, Department of Political Science and International Relations, Bahçeşehir Cyprus University; 6-13-2022; "Turkish-American strategic partnership: is Turkey still a faithful ally?"; Taylor &amp; Francis; https://www.tandfonline.com/doi/abs/10.1080/14683857.2022.2088081?journalCode=fbss20; KL]

American analysts have also raised the question of Turkey’s expulsion from NATO (Carpenter 2019). The suspension of membership rights or the explosion of a member is not clearly stated in NATO’s founding treaty. Turkish policymakers do not consider unilaterally withdrawing from NATO’s collective security umbrella due to its troubled neighbourhood and history with its current allies, Russia and Iran. However, the escalating tension between the US and Turkey and restrictions on security and defence alliance are likely to isolate Turkey from NATO activities. Several NATO allies, including Czechia, Finland, France, Germany, Italy, the Netherlands, Spain, Sweden, the UK, and Canada, have already announced that they have suspended the sale of military equipment to Turkey (BBC News 2019b). After the UK, another NATO member Canada also decided to suspend exports related to drone technology to Turkey on the basis that Turkey provided these technologies to Azeri forces during the Nagorno-Karabakh conflict (Reuters 2020). The US Ambassador to NATO, Kay Bailey Hutchison, underlines that Russia is trying to flip a key member of NATO, and Russia would be one of the main beneficiaries of the destabilization of the alliance and Turkey’s expulsion (Hurriyet Daily News 2018). Turkey was always seen valuable ally and indispensable member of NATO because of its geostrategic significance and military capabilities. It has been argued that alienating Turkey from NATO is not possible for these reasons, but there has been an ongoing Western effort to develop alternative options for Turkey by promoting closer cooperation with Greece, Bulgaria, and Romania (Idiz 2021). With increasing isolation from NATO, Turkey would continue strengthening its military ties with Russia. Erdoğan has already confirmed that Turkey will jointly produce S-500 defence systems with Russia (Reuters 2019). He underlined that ‘if the US. refuses to sell F-35 fighter jets, then Turkey turns to other options’ (Hurriyet Daily News 2019b). Turkey’s removal from the F-35 program might likely force Turkey to look for other options, possibly Russian Su-34 and Su-57 fighter jets (Groll and Seligman 2019). In this case, Turkey’s over-reliance on Russia will reduce its capacity to formulate independent foreign policies and pursue its national interest. Russia is increasingly becoming Turkey’s neighbour, which might be a problem for Turkey in the mid-to-long term.5 Turkish policymakers are aware of this dilemma, and instead of opting for Russian jets (compensate F-35), in October 2021, Turkey has requested to buy 40 new F-16 fighter jets and 80 modernization kits for its existing air forces from the US (Pamuk and Stone 2021). The American attitude will be decisive in Turkey’s return to the Western fold or further isolation from the alliance.

Following the American withdrawal and Turkish military incursions in Syria, French President Emmanuel Macron criticized the lack of coordination between NATO allies. He expressed his frustration by stating that NATO is experiencing ‘brain death’ (Solletty 2019). Biden calls for a renewed commitment to multilateralism and strengthening the transatlantic ties that were weakened during Trump’s America first policy. Pentagon defines the current security environment by identifying China as a ‘pacing challenge’ within the strategic competition, whereas Russia has been identified as a significant but ‘lesser threat’ to US interests and security (Vergun 2021). The Biden administration re-embraces the ‘pivot to Asia’ rhetoric introduced by the Obama administration in 2011, referring to the development of a grand strategy to deal with the North Korean threat and China (Manyin et al. 2012). However, Russia’s full-scale invasion of Ukraine demonstrates that currently, Russia poses a greater risk to the rule-based international system, and the American pivot will be towards Russia and Europe. Strengthening transatlantic ties is not possible without taking Turkey back from Russia. Turkey, NATO’s second-largest army and third most populous member, has a geostrategic significance due to its proximity to Russia and the Middle East. It would help limit Russian expansion in several regions, including the MENA, Eastern Mediterranean and the Black Sea. Therefore, bringing back Turkey to the Western camp is important to contain the US adversaries in multiple regions since Turkey actively fought on the opposing side of Russia in those regions. Turkey actively has pursued increasingly military engagement abroad; it has launched four major military operations in Syria, deployed military troops in Qatar and Somalia, introduced the Blue Homeland doctrine, and expanded its defence exports. Turkey’s indigenous unmanned combat aerial vehicle (UCAV) capabilities are an element of Turkey’s changing defence and security policies, as its drone capabilities are progressing rapidly. Israel was the main contractor supplying unmanned aerial vehicles (UAV) to the Turkish military (Defense Industry Daily 2011). However, with the flotilla crisis in 2010, Turkish-Israeli diplomatic relations collapsed, and Turkey has started to focus on developing its domestic drone program UCAV fleet known as the Bayraktar TB2. The Bayraktar TB2 has been operative since 2015 and became a valuable strategic asset in Turkey’s counterterrorism operations against the PKK in Northern Iraq, Syria and Libya. In recent years, Turkey’s drone power gained attention internationally. The Bayraktar TB2 armed UAVs significantly contributed to Azerbaijan’s victory (Kınık and Çelik 2021), and Ukraine has been relying on Turkish-made drones to target Russian targets (Forrest and Malsin 2022), which implies the possibility that Turkey’s indigenous, but ambitious defence industry can be used to balance against Russia.

Turkey did not participate in the EU sanctions against Russia after Russia’s military incursion in 2014 due to economic reasons (Sputnik News 2015), and Turkish authorities declared that Turkey had no intention or plan to join/impose sanctions against Russia following the invasion of Ukraine. Turkish Foreign Minister Mevüt Çavuşoğlu emphasizes the importance of keeping communication channels open and underlines that ‘we are the country that can establish a dialogue on both sides in order to end the war’ (Hurrriyet Daily News 2022). Turkish authorities are willing to continue cooperation with Russia due to trade and energy dependency and the national security interests in Syria. A successful balancing strategy between Russia and the West in Ukraine might give Erdoğan a win in the international arena that he desperately needs for the upcoming 2023 general election. Turkey has adopted a ‘strategic balancer’ position, and it is trying to balance its NATO alliance by cooperating with emerging non-Western partners in Eurasia, including Russia, Iran, and China (Flanagan et al. 2020, 47). While Turkey’s manoeuvre is perceived as a threat to the Western alliance, Turkey’s competition with Russia in various regions could also be an asset for NATO to balance against Russia in the long run.

Recently, Turkey has been signalling to block NATO’s expansion and inclusion of the two Nordic countries, Finland and Sweden, in the security alliance. Turkey’s concerns regarding accepting new members are based on these two countries’, especially Sweden’s, support for terror organizations, referring to the PKK. Turkey insists that both countries should amend their terror laws. Turkey’s threat to veto NATO’s enlargement is consistent with policy-making elites’ security-first rhetoric. Russian aggression and NATO’s enlargement agenda become an opportunity for Turkey to pressure the two to revise their law, stop harbouring terrorist groups, and pressure NATO allies to lift sanctions on Turkey’s defence industry. Turkey’s objection to the transatlantic alliance enlargement will likely dominate the upcoming NATO Summit in Madrid. As the NATO members prioritize strengthening the alliance in the wake of the Russian invasion of Ukraine, Turkey’s security-driven discourse and possible veto for new members might lead to re-questioning Turkey’s faithful ally role.

Conclusion

Syrian civil war and regional instabilities as independent variables have been incorporated with unit-level intervening variables (Turkish decision-making elites’ threat perceptions, nationalism, societal cohesion, and AKP’s vulnerability to domestic instabilities) and eventually have shaped the Turkish foreign policy formulation and outcomes. The analysis of intervening variables helps to understand how Turkish policymakers extracted and mobilized state resources to respond to systemic pressure and identified threats in Turkey’s immediate neighbourhood. Both the internal and external factors have been influential in the country’s security-first policy and military activism, deteriorating relations with the US, and competitive-cooperation with Russia. Turkish policymakers have prioritized Turkey’s national security over its faithful ally status. The first delivery of S-400s and the US decision to remove Turkey from the F-35 program were among the most significant ruptures in Turkish-American relations. Any expectation of achieving a mutually acceptable solution on S-400s and the YPG seems impossible anytime soon. Turkey still insists on keeping S-400s despite its expulsion from the F-35 program. The US decision to continue its support to the YPG will push Turkey to make new deals with Russia to get a second battery of S-400s. The development in Ukraine is a game-changer for Turkish-American and Turkish-Russian relations.

The visible shift in Turkish foreign policy behaviour in the recent decade cannot be interpreted as a shift in Turkey’s overall foreign policy orientation. The AKP-MHP policy-making elites aim to reposition Turkey in the changing geopolitical realities by adopting a balancing strategy to manage the country’s relations with the US and Russia while maintaining power at home. Turkey’s NATO membership is still the main axis of Turkish foreign policy. Russian challenge to the rule-based liberal international order is likely to end discussions regarding Turkey’s NATO membership at a time when the Western alliance cannot afford any friction among NATO members. The solidarity among NATO allies will be the most critical concern among the Western countries in the following years. Thus, despite Erdoğan’s increasing authoritarianism and acquisition of S-400s Biden administration is likely to avoid escalating tension with Turkey. Turkey’s geostrategic significance for NATO missions makes it an indispensable ally. Turkey hosts the Incirlik airbase and Kürecik radar base and controls the straits of the Bosporus and the Dardanelles. Recently initiated Blue Homeland doctrine to demonstrate Turkey’s willingness to strengthen the country’s naval forces in the Mediterranean and the Black Sea, which can help balance against Russian revisionism. Turkey’s cooperation with Russia is on a knife-edge relationship, so NATO plays and will continue to play a central role in Turkey’s national security strategy. Turkey’s isolation from NATO activities will force Turkey to find alternative security and defence alliances with other actors. It will likely continue to deepen its military ties with Russia by being part of the S-500 supply chain and purchasing Russian Su-34 or Su-57 fighter jets. At this point, Turkey still can be a member of NATO, but without having coordination in military activities, neither Turkey nor NATO members will have a strong commitment to supporting each other’s policies as a faithful ally in the form of a collective security alliance.

#### Improving relations solves every threat. The Strategic Mechanisms thumps DAs and is a force multiplier, but it’s only a first step.

Coşkun 22 [Alper Coşkun; senior fellow within the Europe Program at the Carnegie Endowment for International Peace. His research focuses on Turkish foreign policy, especially in relation to the United States and Europe; 5-12-2022; "Making the New U.S.-Turkey Strategic Mechanism Meaningful"; Carnegie Endowment for International Peace; https://carnegieendowment.org/2022/05/12/making-new-u.s.-turkey-strategic-mechanism-meaningful-pub-87117; KL]

As the war between Russia and Ukraine grinds on and as the need to maintain a united front against Moscow grows, Turkey and the United States are seeking to put their long-troubled relationship on a better path. The new U.S.-Turkey Strategic Mechanism, announced in early April 2022, is a promising (but tentative) step forward.

The mechanism grew out of an understanding reached between Turkish President Recep Tayyip Erdoğan and U.S. President Joe Biden during their meeting on the margins of the October 2021 G20 summit in Rome. Though the idea is said to belong to Biden, the U.S. readout after the meeting lacked any reference to the mechanism, whereas it was the highlight of the Turkish narrative. This difference in emphasis initially triggered rumors that the United States might be dragging its feet.

After the initiative was announced, U.S. Under Secretary of Commerce for International Trade Marisa Lago visited Turkey to explore opportunities in commercial relations and to discuss how Turkey’s Russia-dependent energy mix could be diversified. Turkish Foreign Minister Mevlüt Çavuşoğlu will travel to the United States to meet with U.S. Secretary of State Antony Blinken on May 18 in the first cabinet-level bilateral visit between the two countries since the Biden administration took office. The initial plans had been to have this meeting in Washington, DC, but the venue has been moved to New York, and the program has been curtailed, reportedly at the behest of the United States and probably in reaction to the conviction of Turkish philanthropist Osman Kavala. While the process hasn’t been derailed, this experience serves as a reminder that the mechanism is vulnerable to different dynamics. Its sustainability and potential to have a positive impact depend on Ankara and Washington making the right choices to facilitate and not undermine policy convergences.

Turkish and American sources talk of the Strategic Mechanism as a structured platform in which all matters can be discussed, with an emphasis on advancing practical bilateral cooperation. The level of ambition that Ankara and Washington will set for the mechanism is yet to be seen and will be important, particularly in view of the failure of some past attempts. The two governments established working groups in 2018 to resolve disputes on consular affairs, Syria policy, and Turkey’s purchase of the Russian S-400 air defense system, but these efforts failed to deliver results and were quickly forgotten. The United States had been reluctant to go forward with the idea at the time, and the lesson from that experience is that, unless the parties have a shared sense of understanding of and joint commitment to the process, its chances of success are slim.

If the Strategic Mechanism is to avoid the fate of the 2018 working groups, Washington and Ankara will need to invest seriously in the process and display real political ownership; agree on clear, shared, and diverse objectives; and simultaneously work to resolve or at least minimize their bilateral disputes.

DEMONSTRATING POLITICAL OWNERSHIP

The mechanism will be dead on arrival unless there is shared commitment in Ankara and Washington. Geopolitical considerations are currently driving this commitment in both countries. Russia’s brazen war in Ukraine and the global divide of systemic rivalry have affected how Turkey and the United States view each other. These events have changed their calculus in favor of closer relations and, in turn, have nurtured the idea of such a mechanism.

For Turkey, balancing Russia has consistently been a consideration. From Ankara’s perspective, the reality is that its security, deterrence, and economic livelihood are bolstered by its membership in NATO, its alliance with the United States, and its albeit shaky inclusion nowadays in the family of liberal democracies. Meanwhile, the Turkish economy is in dire straits as the country’s 2023 parliamentary and presidential elections loom on the horizon, forcing the government into looking for international success stories. The United States, on the other hand, is grappling with the fact that Turkey is a significant geopolitical middle power in its immediate region and beyond. Having Turkey as an ally has started to matter more again. In short, realpolitik calculations are at play for both sides.

For the purposes of optics and practicality, the Strategic Mechanism would benefit from being designed and seen as something more than a bureaucratic exercise. For this to happen, it needs a meaningful political embrace from both sides. Underscoring the mechanism’s importance with a meeting between the two countries’ presidents would give it a big boost. It is no secret that the Biden administration has been cold-shouldering Turkey. This has been evident in the choice Biden and his senior team have made to limit their interactions with their Turkish counterparts, something that Erdoğan has publicly lamented.

U.S. officials have already spoken of the possibility of such a meeting on the mechanism, and Turkey would certainly welcome the idea. The two presidents have only met twice so far since Biden took office, with both encounters on the margins of international meetings. The same arrangement could be made, for example, during the upcoming UN General Assembly meeting in New York in September 2022. The direct involvement of Erdoğan and Biden would give the mechanism good optics, add impetus to the initiative, and (maybe even more importantly) perhaps restrain potential spoilers on either side.

SETTING SHARED OBJECTIVES

U.S.-Turkey relations have deteriorated seriously since the early 2000s, starting with differences over the 2003 U.S. invasion of Iraq. The tenor of bilateral ties has mostly been on a downward trajectory since. An accumulated host of disagreements have kept a damper on the relationship, including on topics like Syria policy, Washington’s half-hearted reaction to the 2016 coup attempt in Turkey, the unfettered ability of the Gulen movement (which Ankara holds accountable for this failed attempt) to still function in the United States, Ankara’s decision to purchase Russia’s S-400 air defense system and ensuing U.S. sanctions, and the overall unhappiness in Washington with the incremental dismantling of democratic governance in Turkey.

A byproduct of the regression in U.S.-Turkey relations has been a decrease in bilateral exchanges, which is slowly eroding valuable human networks and taking a toll on the culture of cooperation between the two countries. The Strategic Mechanism can reverse this trend by breaking the numbing effect that disagreements have had on U.S.-Turkey ties. But for this to happen, Washington and Ankara will need to set clear, mutually agreed-on objectives and diversify their objectives to avoid simply trying to address the well-worn agenda of existing disputes.

The 2018 working groups exemplified the damaging effects of failing to achieve these goals. This time, the idea behind the Strategic Mechanism is different. Stimulating an agenda of practical cooperation, without ruling out the possibility of discussing disagreements, is a good way to strike a balance.

Ukraine will be a natural topic of discussion within the mechanism. This should be more than an act of ritualistic exchange and should instead focus on concrete deliverables, including for the post-conflict stage. The future Euroatlantic security architecture and Russia’s role therein and bilateral U.S.-Turkey collaboration in rebuilding and rehabilitating war-torn Ukraine are two themes that come to mind. Meanwhile, the departure of U.S. firms from Russia and the need for at least some of them to relocate their investments and production lines, as well as the realization about the importance of reliable supply chains, create new dynamics where Turkey can bring added value. Given that the United States has become Turkey’s second-largest gas supplier after Russia and that bilateral U.S.-Turkey trade posted a 30 percent increase last year to reach record highs, energy and trade are two other promising areas of cooperation that the Strategic Mechanism can help consolidate.

The list can be extended. Turkey’s ambitious outreach to Africa and its growing footprint on the continent, as well as its renewed efforts to mend fences with Armenia, present further opportunities of convergence with the United States. And despite some serious differences over Syria policy, Turkish and U.S. officials need to continue exploring options for facilitating a political settlement that would allow for the voluntary return of Syrian refugees to their home country.

If Ankara and Washington can advance cooperation in some of these areas, that would qualitatively improve a U.S.-Turkey partnership that has traditionally been set in a straitjacket of sometimes divergent security and defense interests. The Strategic Mechanism can help broaden this relationship and make it more resilient. The proposal’s added value would lie in introducing structure and continuity to different strands of engagement between the two countries and in its potential to swiftly elevate ripe schemes to political decisionmakers for their endorsement. In short, if the objectives are set right, the Strategic Mechanism could hasten both the incubation and implementation of useful ideas.

REDUCING THE POISONING EFFECTS OF DISAGREEMENTS

If the Strategic Mechanism is to help Turkey and the United States engage more deeply and enhance practical cooperation, something will have to be done in tandem to mitigate the poisoning effects of bilateral disagreements. This is where things get more complicated, and there is a mismatch between Ankara and Washington in terms of not only policy substance but also methods of diplomatic negotiations.

First, while Russia’s war on Ukraine and its generally aggressive posturing, as well as related geopolitical dynamics, have created a convergence between Ankara and Washington, there is also the risk that both sides may believe their own hand has been strengthened at the expense of the other. In fairness, they both have valid reasons to think so. Turkey is inclined to focus on and overstate the value of its geopolitical stock, which has clearly appreciated in the wake of the crisis, while the United States would prefer to stress the need for an awakening in Ankara on the risks associated with entanglement with and exposure to Russia. Blinken alluded to U.S. expectations in general terms while testifying before Congress in late April, when he spoke of the strategic opportunities that U.S. officials see in the ways various countries are rethinking the now more evident risks associated with dependencies on Russia. Both Turkey and the United States should be careful not to overplay their hands at this time of opportunity. If Turkey and Washington are to resolve, or at least mitigate, the negative effects of their differences, their point of departure cannot be that each side feels it has the upper hand and can now impose its will on the other. They will both need to compromise.

Second, while it is wise to spare the Strategic Mechanism of the burden of pointedly focusing on bilateral disagreements, assuming these matters can simply be set aside would be a mistake. The poisonous seeping effects of the problems weighing down the relationship do not afford the luxury of time. That is the underlying risk associated with seemingly practical solutions like embracing transactionalism, attempting compartmentalization, and focusing on low-hanging fruit while leaving problems on the back burner. Such an attempt would mean sleepwalking toward a future in which current problems will probably become more ossified and solutions will be harder to find. Despite such risks, Washington seems more inclined to wait things out, mostly because of its reluctance to engage in a process that is limited to rehashing arguments that have already been made to no effect. Turkey, on the other hand, seems ready to continue the debate, no matter what. The gap that needs to be bridged here involves identifying new common ground to move on. That is the incentive both sides need, and in Washington’s case, it is seen as a prerequisite. But the onus to create these conditions cannot fall on one side alone. It must be a mutual endeavor.

Two priorities are the S-400 conundrum and differences in Syria. On the first point, while Turkey tested the Russian-acquired system in late 2020 as part of the acquisition process, Ankara has chosen not to bring the system online yet. The Turkish government should hold this posture. It should concurrently stop amplifying the message that it retains the right to acquire additional systems from Russia and refrain from posturing through such statements. Political and operational realities emerging from the war in Ukraine should already have put an end to the debate over the expediency of adding Russian weapons systems to Turkey’s defense inventory. Many useful ideas on how to overcome the S-400 problem have already been put forward, and any solution will need to involve a workable formula to meet or work around the requirement in the U.S. National Defense Authorization Act calling for Turkey’s nonpossession of the system as a condition for sanctions to be lifted. Progress on this and also on Turkey’s request to purchase forty state-of-the-art F-16 fighter jets and eighty modernization kits for its existing aircraft would mark a significant breakthrough in bilateral relations and would have positive ripple effects. There are encouraging signs that the F-16 issue may slowly be evolving in the right direction.

It will be equally important to find a way forward in Syria. The perception that the United States continues to supply Kurdish elements that Ankara believes are associated with the Kurdistan Workers’ Party (PKK), a separatist militant group that targets Turkey and that is listed as a terrorist organization in the United States and the EU, is taking a heavy toll on Turkish sentiments toward the United States. The harm this is doing to bilateral relations cannot be overstated. While the United States may have internally normalized this state of affairs, the same cannot be expected of Turkey. Nor would that expectation correspond to the repeated assurances the United States has given Turkey in the past. When U.S. officials chose to begin this engagement in Syria, they reassured Turkey repeatedly that the arrangement was temporary, transactional, and tactical— geared solely to fighting the threat of the self-proclaimed Islamic State. This would be the right moment for the United States to start considering how to wind down its engagement with these Kurdish elements in Syria and for Turkey to come forward with practical solutions that address overriding U.S. security interests in Syria on the threat posed by the Islamic State, though there is little visible appetite in Washington to do so now.

Another relevant factor is the state of democracy and the rule of law in Turkey. This will have a bearing on the type of engagement Turkey and the United States can achieve through the Strategic Mechanism and beyond. The view that Turkey is backsliding on its human rights and rule of law standards is a fundamental problem. It is severely undermining Ankara’s image and interests, including on the economic front in terms of the country’s perceived investment climate. Turkey’s quest to establish a solid international reputation cannot be achieved when the Turkish government, for instance, disregards its obligations under international law and under its own constitution to uphold decisions by the European Court of Human Rights. As Turkey speaks of a new era in its foreign policy and tries to portray itself in a positive light as a responsible and reliable international actor, it cannot concurrently tighten the screws internally on the Turkish people’s freedoms and human rights or flout its relevant responsibilities. This is particularly true as the temptation grows to define the global order by delineating between democratic states and nondemocratic ones. Turkey’s aspirations and actions should correspond to those befitting truly democratic states. This would strengthen Turkey’s hand in every respect and augment its ability to make the most of the Strategic Mechanism with the United States.

THE GLASS IS HALF FULL

The U.S.-Turkey Strategic Mechanism is no silver bullet, and one should not expect any miracles. Rebuilding trust between Ankara and Washington and changing accumulated negative perceptions will take patience and concrete action. By consolidating different strands of bilateral engagement under shared political ownership, the Strategic Mechanism can be a useful force multiplier. Despite skeptics on both sides and against all odds, the glass is half full in U.S.-Turkey relations: if used wisely and in conjunction with the right policy choices, the Strategic Mechanism can help bolster this momentum.

## Uniqueness CP

#### The counterplan causes Baltic, Greece, and Taiwan war. Goes nuclear!

Jensen 7-15 [Stephan Jensen, former Officer in the Norwegian Army; 6-16-2022; "If Europe Wants Peace, It Must Prepare for More War"; Quillette; https://quillette.com/2022/07/15/if-europe-wants-peace-it-must-prepare-for-more-war/; KL]

Should NATO not receive the necessary upkeep—whether through the US stepping back or European countries failing to re-build their militaries in the near future—a number of unfortunate scenarios become more likely. First and foremost, Russian aggression beyond Ukraine is entirely dependent on Putin or his successor believing they might be successful. This is a situation which only becomes possible if Europe fails to adequately rebuild its militaries.

Other threats might also emerge. If NATO ceases to be a powerful alliance, Erdoğan, for example, might gravitate away from it and towards Russia and China instead. This is especially worrisome as Turkey has revanchist claims on territory in Greece, a fellow member of NATO. Orbán, too, has prevaricated about whether Hungary’s place is with the EU and NATO or Putin’s Russia. If a realignment was accompanied by Russia finally succeeding in Ukraine—a scenario which becomes far more likely if Western support begins to fall away—NATO-members Bulgaria and Romania could quite literally be “boxed in” by Russia, Turkey, and Hungary.

In an extreme worst-case scenario, one might imagine a de-facto alliance between Russia, China, Turkey, and other minor powers; and a NATO weakened by a lack of European defence investment and American prevarication over their commitment to the alliance. In such a situation, war breaking out simultaneously over Russian claims in the Baltics, Turkish claims in the Aegean, and Chinese claims to Taiwan become a real possibility—precisely because it would be far from obvious that the West would prevail.

More importantly, even if Europe were to win such a war and nuclear apocalypse were to be avoided, it would still be a catastrophic event. In the least-worst case, hundreds of thousands of people would die, vast sums of wealth and prosperity would be destroyed, and the lives of millions of survivors would be scarred by the experiences of war.

# AT: T

## T The = All of Nato

### 2ac---t “the”

#### We meet – all of the North Atlantic Treaty Organization can participate – if we don’t meet then no aff does because any NATO member could always say no

#### We meet – ‘in’ means a subset of – that means we have to be a subset of NATO’s cyber security

#### “In” means within, not “throughout”

Cullen ’52 [Court of Appeals of Kentucky, Commissioner, Court of Appeals of Kentucky, November 13, 1952, Riehl et al. V. Kentucky unemployment compensation commission; the judgment is affirmed. Rehearing denied; COMBS, J., and SIMS, C. J., dissenting, <http://ky.findacase.com/research/wfrmDocViewer.aspx/xq/fac.19521113_0040095.KY.htm/qx>]

We do not find any ambiguity in KRS 341.070(1). It is our opinion that the key word in the statute is the word 'in,' preceding the words 'each of three calendar quarters', and if the word is accorded its ordinary and common meaning, the statute does not require simultaneous employment. According to Webster's New International Dictionary, the word 'in,' used with relation to a period of time, means 'during the course of.' The same meaning, expressed in another way, would be 'within the limits or duration of.' Employing this meaning, the statute says that an employer is subject to the Act if, during the course of, or within the limits or duration of each of three calendar quarters, he had in covered employment four or more workers, to each of whom the required amount of wages was paid. This clearly means that the employment need not be simultaneous. Obviously, the word 'in' does not mean 'throughout' or 'for the entire period of,' because then there would be no point in adding the requirement of the payment of a minimum of $50 in wages. In these times, no worker employed for a full calendar quarter would be paid less than $50 in wages. The appellant seeks to read into the statute the words 'at the same time,' following the words 'had in covered employment'. There is no justification for this, unless the word 'in' means 'during any one period of time in.' We are not aware of any authority for ascribing such a meaning to the word 'in'.

#### focus on specific assets and vulnerabilities such as in Baltic region is a subset of all NATO cyber security

John M Borky 9-9-2018, "Protecting Information with Cybersecurity," PubMed Central (PMC), https://www.ncbi.nlm.nih.gov/pmc/articles/PMC7122347//DG

In dealing with cybersecurity, risk management is focused on protected assets, threats, vulnerabilities, and risk mitigation using security controls. It begins with risk identification and analysis, which then supports selection of security controls to achieve an acceptable risk level. This, in turn, is the basis for securing approval to operate the system. Accordingly, risk analysis is an essential component of defining security policy and requirements. The goal is to apply security controls intelligently to mitigate the most important risks while preserving an operationally effective, affordable, and supportable system. Risk management continues over the life of a system to deal with changes to the system itself and with the emergence of new vulnerabilities and threats.

#### C/I

#### “The” does not mean “all”---it varies per specific application.

Michael Dewine 15. Attorney General of Ohio. “Gillie v. Law Office of Eric A. Jones, LLC: ON WRIT OF CERTIORARI TO THE UNITED STATES COURT OF APPEALS FOR THE SIXTH CIRCUIT BRIEF FOR THE PETITIONERS. 2015. Lexis //EM

Duties Of The Office.

The Sixth Circuit next read “the duties of the office” to require the person to perform “all duties associated with the office.” Pet. App. 35a. Special counsel, the court added, do not perform all of the Attorney General’s duties. Id.

Yet “the” does not mean “all.” The Dictionary Act uses the definite article to identify the specific duties delegated by the specific authorizing law. Here, that law permits special counsel to perform the debt-collection duties of the Attorney General’s Office. Read otherwise, the Dictionary Act would exclude any inferior officer in an office who could not perform all of the superior’s duties.

#### Prefer it:

1. Overlimiting---excludes swaths of the collaboration lit base
2. Aff ground---country pics decimate the topic, exclude discussion of NATO
3. Precision---cites 6th circuit decisions AND dictionary which is good for plain meaning reasons
4. Abusive counterplans---“the” as “all” means the aff loses to pics out of individual district courts ruling against the plan which compete based off “the” usfg
5. Mixes burdens – makes it so that the aff has to win the say yes debate to prove topicality since any NATO member can say no to any plan
6. Reasonability

### In

#### “In” means within the limits of

Webster’s ‘6 [Merriam Webster Online Dictionary, 2006, <http://www.m-w.com/cgi-bin/dictionary?book=Dictionary&va=in>]

Main Entry: 1in

Pronunciation: 'in, &n, &n

Function: preposition

Etymology: Middle English, from Old English; akin to Old High German in in, Latin in, Greek en

1 a -- used as a function word to indicate inclusion, location, or position within limits <in the lake> <wounded in the leg> <in the summer>

#### Prefer plain meaning.

Scalia ’12 [Antonin Scalia and Bryan Garner; 2012; Justice on the Supreme Court of the United States; American lawyer, lexicographer, and teacher; Reading Law: The Interpretation of Legal Texts, “Ordinary-Meaning Canon,” Ch. 6]

Words are to be understood in their ordinary, everyday meanings—unless the context indicates that they bear a technical sense.

“The enlightened patriots who framed our constitution, and the people who adopted it, must be understood to have employed words in their natural sense, and to have intended what they have said.”

Chief Justice John Marshall,

Gibbons v. Ogden, 22 U.S. (9 Wheat.) 1, 71 (1824).

The ordinary-meaning rule is the most fundamental semantic rule of interpretation.1 It governs constitutions, statutes, rules, and private instruments. Interpreters should not be required to divine arcane nuances or to discover hidden meanings. Justice Joseph Story’s words are as true today as they were when written in the middle of the 19th century, and they are true not just of constitutions but of all other legal instruments:

[E]very word employed in the constitution is to be expounded in its plain, obvious, and common sense, unless the context furnishes some ground to control, qualify, or enlarge it. Constitutions are not designed for metaphysical or logical subtleties, for niceties of expression, for critical propriety, for elaborate shades of meaning, or for the exercise of philosophical acuteness or judicial research. They are instruments of a practical nature, founded on the common business of human life, adapted to common wants, designed for common use, and fitted for common understandings.2

### The

#### The most precise definition of “The” specifies particulars

Supreme Court of Minnesota 12. “State v. Hohenwald”; A10-1986; July 11, 2012; Lexis //BY

With regard to Minn. R. Crim. P. 20.01, the definite article "the" is a word of limitation that indicates a reference to a specific object. The definite article "the" particularizes the subject which it precedes. "The" is used before singular or plural nouns and noun phrases that denote particular, specified persons or things Applying the word "the" as a word of limitation, Rule 20.01 requires the suspension of the proceedings in the then-existing case in which the court orders the suspension, not in an unspecified or indefinite number of cases. The word "the" is a word of limitation, not a word of indefinite or generalizing force. If the drafters of the criminal rules intended to suspend all proceedings brought against a particular criminal defendant, including those not yet in existence, they could have easily used words to that effect by suspending "all criminal proceedings" or "any criminal proceedings." Thus, the most natural reading of Rule 20.01 is that it requires district courts to suspend the proceedings in only the particular case in which it orders the suspension, not in all prospective actions that could possibly arise during the period of suspension.

#### “The” can determine specifics

Supreme Court of Michigan 21. “Ricks v. State”; July 8, 2021; Lexis //BY

In its review of the threshold-eligibility requirements in MCL 691.1755(1), the Court of Appeals aptly recognized that the Legislature repeatedly used the word [\*\*440] "the" in front of "crimes," "charges," and "judgment of conviction" in MCL 691.1755(1)(a) to (c) in setting forth when a plaintiff is eligible for compensation under the WICA. On the other hand, the Legislature uses the word "another" before "criminal offense" in MCL 691.1755(1)(b) and [\*\*\*27] "conviction" in MCL 691.1755(4)—other subsections of MCL 691.1755 that explain when a plaintiff is not eligible for compensation. We have previously defined "the" as a "definite article . . . (used, especially before a noun, with a specifying or particularizing effect, as opposed to the indefinite or generalizing force of the indefinite article a or an)."20Link to the text of the note As an adjective, "another" is defined as "different or distinct from the one first considered"; "some other"; or "being one more in addition to one or more of the same kind."21Link to the text of the note Accordingly, the Legislature's use of "the" before "crimes," "charges," and "judgment of conviction" throughout MCL 691.1755(1)(a) to (c) means those provisions refer to the specific crimes and charges leading to a plaintiff's wrongful conviction and imprisonment that gave rise to a WICA claim. The Legislature's use of "another" before "criminal offense" in MCL 691.1755(1)(b) and "conviction" in MCL 691.1755(4) [\*413] means those provisions refer to some other offense or conviction that is different or distinct from the wrongful conviction and imprisonment, and which therefore does not warrant compensation under the WICA. Thus, MCL 691.1755 reflects the overall structure of the WICA in only providing compensation for the specific crimes, charges, or convictions [\*\*\*28] that the plaintiff was wrongfully convicted of and imprisoned for, and which ultimately form the basis of the WICA claim—not "another" crime, charge, or conviction.

### AT: Kotila

#### Kotila is not good law. It was overruled [that’s the red dot next to the case in the picture below]

Lexis Academic 22//BB

Graphical user interface, text, application, email

Description automatically generated

#### That was because the definition of “the” did violence to common sense

Supreme Court of Kentucky 6. “Matheney v. Commonwealth”; 2002-SC-0920-MR; March 23, 2006; Lexis //BY

In [Kotila v. Commonwealth, 114 S.W.3d 226 (Ky. 2003)](https://advance-lexis-com.proxy.lib.umich.edu/document/?pdmfid=1516831&crid=849d3182-5ba6-4c04-afa9-d06b2d0290dd&pddocfullpath=%2Fshared%2Fdocument%2Fcases%2Furn%3AcontentItem%3A4JJ9-5VM0-TVV9-0200-00000-00&pdcontentcomponentid=7240&pdshepid=urn%3AcontentItem%3A7XW4-F4J1-2NSF-C3VF-00000-00&pdteaserkey=sr5&pditab=allpods&ecomp=rzznk&earg=sr5&prid=ef50c0ae-9882-4e7b-b6fd-23b8257a21e8), this Court held that the version of [KRS 218A.1432(1)(b)](https://advance-lexis-com.proxy.lib.umich.edu/document/?pdmfid=1516831&crid=849d3182-5ba6-4c04-afa9-d06b2d0290dd&pddocfullpath=%2Fshared%2Fdocument%2Fcases%2Furn%3AcontentItem%3A4JJ9-5VM0-TVV9-0200-00000-00&pdcontentcomponentid=7240&pdshepid=urn%3AcontentItem%3A7XW4-F4J1-2NSF-C3VF-00000-00&pdteaserkey=sr5&pditab=allpods&ecomp=rzznk&earg=sr5&prid=ef50c0ae-9882-4e7b-b6fd-23b8257a21e8) then in effect required possession of all the chemicals or equipment necessary to manufacture methamphetamine. Essentially, this Court found that the statute's use of the word[[\*\*5]](https://advance-lexis-com.proxy.lib.umich.edu/document/?pdmfid=1516831&crid=849d3182-5ba6-4c04-afa9-d06b2d0290dd&pddocfullpath=%2Fshared%2Fdocument%2Fcases%2Furn%3AcontentItem%3A4JJ9-5VM0-TVV9-0200-00000-00&pdcontentcomponentid=7240&pdshepid=urn%3AcontentItem%3A7XW4-F4J1-2NSF-C3VF-00000-00&pdteaserkey=sr5&pditab=allpods&ecomp=rzznk&earg=sr5&prid=ef50c0ae-9882-4e7b-b6fd-23b8257a21e8) "the" meant that a person could be convicted under [subpart (1)(b)](https://advance-lexis-com.proxy.lib.umich.edu/document/?pdmfid=1516831&crid=849d3182-5ba6-4c04-afa9-d06b2d0290dd&pddocfullpath=%2Fshared%2Fdocument%2Fcases%2Furn%3AcontentItem%3A4JJ9-5VM0-TVV9-0200-00000-00&pdcontentcomponentid=7240&pdshepid=urn%3AcontentItem%3A7XW4-F4J1-2NSF-C3VF-00000-00&pdteaserkey=sr5&pditab=allpods&ecomp=rzznk&earg=sr5&prid=ef50c0ae-9882-4e7b-b6fd-23b8257a21e8) of the statute only for possession of all the chemicals or equipment (as opposed to "any" or "some" of the chemicals or equipment) for the manufacture of methamphetamine. The Kotila majority based this conclusion on grammatical construction and subsequent statutory enactments by the General Assembly. While attempting to discern the General Assembly's intent by analyzing subsequent legislation, the majority opinion conceded that the precise intent of the General Assembly was ambiguous.

The majority also rejected the applicability of criminal attempt under [KRS 506.010](https://advance-lexis-com.proxy.lib.umich.edu/document/documentlink/?pdmfid=1516831&crid=3a8e040e-84fe-4663-a0f3-ed97f4fd2ad4&pddocfullpath=%2Fshared%2Fdocument%2Fstatutes-legislation%2Furn%3AcontentItem%3A5D87-S411-66PR-P4S2-00000-00&pdcontentcomponentid=7244&pddoctitle=KRS+506.010&pdproductcontenttypeid=urn%3Apct%3A83&pdiskwicview=false&ecomp=4sk8k&prid=849d3182-5ba6-4c04-afa9-d06b2d0290dd) unless all the chemicals or equipment necessary to manufacture methamphetamine were present. Justice Keller concurred in the Court's opinion relating to [KRS 218A.1432(1)(b)](https://advance-lexis-com.proxy.lib.umich.edu/document/?pdmfid=1516831&crid=849d3182-5ba6-4c04-afa9-d06b2d0290dd&pddocfullpath=%2Fshared%2Fdocument%2Fcases%2Furn%3AcontentItem%3A4JJ9-5VM0-TVV9-0200-00000-00&pdcontentcomponentid=7240&pdshepid=urn%3AcontentItem%3A7XW4-F4J1-2NSF-C3VF-00000-00&pdteaserkey=sr5&pditab=allpods&ecomp=rzznk&earg=sr5&prid=ef50c0ae-9882-4e7b-b6fd-23b8257a21e8). However, he believed [[\*603]](https://advance-lexis-com.proxy.lib.umich.edu/document/?pdmfid=1516831&crid=849d3182-5ba6-4c04-afa9-d06b2d0290dd&pddocfullpath=%2Fshared%2Fdocument%2Fcases%2Furn%3AcontentItem%3A4JJ9-5VM0-TVV9-0200-00000-00&pdcontentcomponentid=7240&pdshepid=urn%3AcontentItem%3A7XW4-F4J1-2NSF-C3VF-00000-00&pdteaserkey=sr5&pditab=allpods&ecomp=rzznk&earg=sr5&prid=ef50c0ae-9882-4e7b-b6fd-23b8257a21e8) that [KRS 506.010](https://advance-lexis-com.proxy.lib.umich.edu/document/?pdmfid=1516831&crid=849d3182-5ba6-4c04-afa9-d06b2d0290dd&pddocfullpath=%2Fshared%2Fdocument%2Fcases%2Furn%3AcontentItem%3A4JJ9-5VM0-TVV9-0200-00000-00&pdcontentcomponentid=7240&pdshepid=urn%3AcontentItem%3A7XW4-F4J1-2NSF-C3VF-00000-00&pdteaserkey=sr5&pditab=allpods&ecomp=rzznk&earg=sr5&prid=ef50c0ae-9882-4e7b-b6fd-23b8257a21e8) applied to "defendants who intend to manufacture methamphetamine and who undertake 'substantial steps' towards manufacturing methamphetamine by knowingly accumulating materials necessary to do so, but who are apprehended before they can complete the [KRS 218A.1432(1)(b) [\*\*6]](https://advance-lexis-com.proxy.lib.umich.edu/document/?pdmfid=1516831&crid=849d3182-5ba6-4c04-afa9-d06b2d0290dd&pddocfullpath=%2Fshared%2Fdocument%2Fcases%2Furn%3AcontentItem%3A4JJ9-5VM0-TVV9-0200-00000-00&pdcontentcomponentid=7240&pdshepid=urn%3AcontentItem%3A7XW4-F4J1-2NSF-C3VF-00000-00&pdteaserkey=sr5&pditab=allpods&ecomp=rzznk&earg=sr5&prid=ef50c0ae-9882-4e7b-b6fd-23b8257a21e8) Manufacturing Methamphetamine offense by knowingly possessing all of the chemicals or all of the equipment necessary to manufacture methamphetamine." [Kotila, 114 S.W.3d at 251](https://advance-lexis-com.proxy.lib.umich.edu/document/?pdmfid=1516831&crid=849d3182-5ba6-4c04-afa9-d06b2d0290dd&pddocfullpath=%2Fshared%2Fdocument%2Fcases%2Furn%3AcontentItem%3A4JJ9-5VM0-TVV9-0200-00000-00&pdcontentcomponentid=7240&pdshepid=urn%3AcontentItem%3A7XW4-F4J1-2NSF-C3VF-00000-00&pdteaserkey=sr5&pditab=allpods&ecomp=rzznk&earg=sr5&prid=ef50c0ae-9882-4e7b-b6fd-23b8257a21e8) (Keller, J., concurring in part and dissenting in part).

Chief Justice Lambert authored a dissent, which was joined by Justice Wintersheimer. Chief Justice Lambert argued that if the General Assembly had intended the statute to be construed as the majority did, "it would surely have used the word 'all' rather than the more general 'the.'" [Kotila, 114 S.W.3d at 256](https://advance-lexis-com.proxy.lib.umich.edu/document/?pdmfid=1516831&crid=849d3182-5ba6-4c04-afa9-d06b2d0290dd&pddocfullpath=%2Fshared%2Fdocument%2Fcases%2Furn%3AcontentItem%3A4JJ9-5VM0-TVV9-0200-00000-00&pdcontentcomponentid=7240&pdshepid=urn%3AcontentItem%3A7XW4-F4J1-2NSF-C3VF-00000-00&pdteaserkey=sr5&pditab=allpods&ecomp=rzznk&earg=sr5&prid=ef50c0ae-9882-4e7b-b6fd-23b8257a21e8) (Lambert, C.J., dissenting). One member of the Kotila majority has subsequently admitted that he "was seduced by a metaphysical infatuation which led to an absurdity" and concluded that Kotila "does violence to the concept of common sense." [Fulcher v. Commonwealth, 149 S.W.3d 363, 381 (Ky. 2004)](https://advance-lexis-com.proxy.lib.umich.edu/document/?pdmfid=1516831&crid=849d3182-5ba6-4c04-afa9-d06b2d0290dd&pddocfullpath=%2Fshared%2Fdocument%2Fcases%2Furn%3AcontentItem%3A4JJ9-5VM0-TVV9-0200-00000-00&pdcontentcomponentid=7240&pdshepid=urn%3AcontentItem%3A7XW4-F4J1-2NSF-C3VF-00000-00&pdteaserkey=sr5&pditab=allpods&ecomp=rzznk&earg=sr5&prid=ef50c0ae-9882-4e7b-b6fd-23b8257a21e8) ([Graves, J.](https://advance-lexis-com.proxy.lib.umich.edu/document/?pdmfid=1516831&crid=849d3182-5ba6-4c04-afa9-d06b2d0290dd&pddocfullpath=%2Fshared%2Fdocument%2Fcases%2Furn%3AcontentItem%3A4JJ9-5VM0-TVV9-0200-00000-00&pdcontentcomponentid=7240&pdshepid=urn%3AcontentItem%3A7XW4-F4J1-2NSF-C3VF-00000-00&pdteaserkey=sr5&pditab=allpods&ecomp=rzznk&earg=sr5&prid=ef50c0ae-9882-4e7b-b6fd-23b8257a21e8), dissenting).

In Fulcher, despite the fact that the defendant possessed a plethora of equipment and chemicals to make methamphetamine, the Court held that since there was no evidence of sodium metal or lithium, the defendant did not possess all the chemicals necessary to manufacture[[\*\*7]](https://advance-lexis-com.proxy.lib.umich.edu/document/?pdmfid=1516831&crid=849d3182-5ba6-4c04-afa9-d06b2d0290dd&pddocfullpath=%2Fshared%2Fdocument%2Fcases%2Furn%3AcontentItem%3A4JJ9-5VM0-TVV9-0200-00000-00&pdcontentcomponentid=7240&pdshepid=urn%3AcontentItem%3A7XW4-F4J1-2NSF-C3VF-00000-00&pdteaserkey=sr5&pditab=allpods&ecomp=rzznk&earg=sr5&prid=ef50c0ae-9882-4e7b-b6fd-23b8257a21e8) methamphetamine. In addition, since there were no mixing bowls, stirring devices or pliers, the defendant also failed to possess all the equipment necessary to manufacture methamphetamine.

This Court has struggled with the effects of Kotila from day one. This is clear from the fact that the bright line rule of Kotila survived for only about six months. In [Varble v. Commonwealth, 125 S.W.3d 246, 254 (Ky. 2004)](https://advance-lexis-com.proxy.lib.umich.edu/document/?pdmfid=1516831&crid=849d3182-5ba6-4c04-afa9-d06b2d0290dd&pddocfullpath=%2Fshared%2Fdocument%2Fcases%2Furn%3AcontentItem%3A4JJ9-5VM0-TVV9-0200-00000-00&pdcontentcomponentid=7240&pdshepid=urn%3AcontentItem%3A7XW4-F4J1-2NSF-C3VF-00000-00&pdteaserkey=sr5&pditab=allpods&ecomp=rzznk&earg=sr5&prid=ef50c0ae-9882-4e7b-b6fd-23b8257a21e8), this Court upheld a conviction under [KRS 218A.1432(1)(b)](https://advance-lexis-com.proxy.lib.umich.edu/document/?pdmfid=1516831&crid=849d3182-5ba6-4c04-afa9-d06b2d0290dd&pddocfullpath=%2Fshared%2Fdocument%2Fcases%2Furn%3AcontentItem%3A4JJ9-5VM0-TVV9-0200-00000-00&pdcontentcomponentid=7240&pdshepid=urn%3AcontentItem%3A7XW4-F4J1-2NSF-C3VF-00000-00&pdteaserkey=sr5&pditab=allpods&ecomp=rzznk&earg=sr5&prid=ef50c0ae-9882-4e7b-b6fd-23b8257a21e8) where all the chemicals except anhydrous ammonia and all the equipment except for a filter were present. The Court held that "the odor of anhydrous ammonia" and a "filter of unspecified nature and a dust filter mask" were sufficient evidence to satisfy Kotila. [Id. at 254](https://advance-lexis-com.proxy.lib.umich.edu/document/?pdmfid=1516831&crid=849d3182-5ba6-4c04-afa9-d06b2d0290dd&pddocfullpath=%2Fshared%2Fdocument%2Fcases%2Furn%3AcontentItem%3A4JJ9-5VM0-TVV9-0200-00000-00&pdcontentcomponentid=7240&pdshepid=urn%3AcontentItem%3A7XW4-F4J1-2NSF-C3VF-00000-00&pdteaserkey=sr5&pditab=allpods&ecomp=rzznk&earg=sr5&prid=ef50c0ae-9882-4e7b-b6fd-23b8257a21e8). Chief Justice Lambert remarked that the holding in Varble represented "a significant departure from the bright line rule announced in Kotila." [Id. at 257](https://advance-lexis-com.proxy.lib.umich.edu/document/?pdmfid=1516831&crid=849d3182-5ba6-4c04-afa9-d06b2d0290dd&pddocfullpath=%2Fshared%2Fdocument%2Fcases%2Furn%3AcontentItem%3A4JJ9-5VM0-TVV9-0200-00000-00&pdcontentcomponentid=7240&pdshepid=urn%3AcontentItem%3A7XW4-F4J1-2NSF-C3VF-00000-00&pdteaserkey=sr5&pditab=allpods&ecomp=rzznk&earg=sr5&prid=ef50c0ae-9882-4e7b-b6fd-23b8257a21e8) (Lambert, C.J., concurring).

Additionally, with Justice Graves's express disavowal of Kotila in his dissent in [Fulcher](https://advance-lexis-com.proxy.lib.umich.edu/document/?pdmfid=1516831&crid=849d3182-5ba6-4c04-afa9-d06b2d0290dd&pddocfullpath=%2Fshared%2Fdocument%2Fcases%2Furn%3AcontentItem%3A4JJ9-5VM0-TVV9-0200-00000-00&pdcontentcomponentid=7240&pdshepid=urn%3AcontentItem%3A7XW4-F4J1-2NSF-C3VF-00000-00&pdteaserkey=sr5&pditab=allpods&ecomp=rzznk&earg=sr5&prid=ef50c0ae-9882-4e7b-b6fd-23b8257a21e8), four members of this Court have cast votes that necessarily demonstrate their disagreement with Kotila's[[\*\*8]](https://advance-lexis-com.proxy.lib.umich.edu/document/?pdmfid=1516831&crid=849d3182-5ba6-4c04-afa9-d06b2d0290dd&pddocfullpath=%2Fshared%2Fdocument%2Fcases%2Furn%3AcontentItem%3A4JJ9-5VM0-TVV9-0200-00000-00&pdcontentcomponentid=7240&pdshepid=urn%3AcontentItem%3A7XW4-F4J1-2NSF-C3VF-00000-00&pdteaserkey=sr5&pditab=allpods&ecomp=rzznk&earg=sr5&prid=ef50c0ae-9882-4e7b-b6fd-23b8257a21e8) holding regarding the application of [KRS 506.010](https://advance-lexis-com.proxy.lib.umich.edu/document/?pdmfid=1516831&crid=849d3182-5ba6-4c04-afa9-d06b2d0290dd&pddocfullpath=%2Fshared%2Fdocument%2Fcases%2Furn%3AcontentItem%3A4JJ9-5VM0-TVV9-0200-00000-00&pdcontentcomponentid=7240&pdshepid=urn%3AcontentItem%3A7XW4-F4J1-2NSF-C3VF-00000-00&pdteaserkey=sr5&pditab=allpods&ecomp=rzznk&earg=sr5&prid=ef50c0ae-9882-4e7b-b6fd-23b8257a21e8) (Criminal Attempt) to methamphetamine manufacturing offenses. See [Kotila, 114 S.W.3d at 249](https://advance-lexis-com.proxy.lib.umich.edu/document/?pdmfid=1516831&crid=849d3182-5ba6-4c04-afa9-d06b2d0290dd&pddocfullpath=%2Fshared%2Fdocument%2Fcases%2Furn%3AcontentItem%3A4JJ9-5VM0-TVV9-0200-00000-00&pdcontentcomponentid=7240&pdshepid=urn%3AcontentItem%3A7XW4-F4J1-2NSF-C3VF-00000-00&pdteaserkey=sr5&pditab=allpods&ecomp=rzznk&earg=sr5&prid=ef50c0ae-9882-4e7b-b6fd-23b8257a21e8) (Keller, J., concurring in part and dissenting in part); [id. at 256](https://advance-lexis-com.proxy.lib.umich.edu/document/?pdmfid=1516831&crid=849d3182-5ba6-4c04-afa9-d06b2d0290dd&pddocfullpath=%2Fshared%2Fdocument%2Fcases%2Furn%3AcontentItem%3A4JJ9-5VM0-TVV9-0200-00000-00&pdcontentcomponentid=7240&pdshepid=urn%3AcontentItem%3A7XW4-F4J1-2NSF-C3VF-00000-00&pdteaserkey=sr5&pditab=allpods&ecomp=rzznk&earg=sr5&prid=ef50c0ae-9882-4e7b-b6fd-23b8257a21e8) (Lambert, C.J., dissenting in part, joined by [Wintershiemer, J.); Fulcher v. Commonwealth, 149 S.W.3d 363, 381 (Ky. 2004)](https://advance-lexis-com.proxy.lib.umich.edu/document/?pdmfid=1516831&crid=849d3182-5ba6-4c04-afa9-d06b2d0290dd&pddocfullpath=%2Fshared%2Fdocument%2Fcases%2Furn%3AcontentItem%3A4JJ9-5VM0-TVV9-0200-00000-00&pdcontentcomponentid=7240&pdshepid=urn%3AcontentItem%3A7XW4-F4J1-2NSF-C3VF-00000-00&pdteaserkey=sr5&pditab=allpods&ecomp=rzznk&earg=sr5&prid=ef50c0ae-9882-4e7b-b6fd-23b8257a21e8) ([Graves, J.](https://advance-lexis-com.proxy.lib.umich.edu/document/?pdmfid=1516831&crid=849d3182-5ba6-4c04-afa9-d06b2d0290dd&pddocfullpath=%2Fshared%2Fdocument%2Fcases%2Furn%3AcontentItem%3A4JJ9-5VM0-TVV9-0200-00000-00&pdcontentcomponentid=7240&pdshepid=urn%3AcontentItem%3A7XW4-F4J1-2NSF-C3VF-00000-00&pdteaserkey=sr5&pditab=allpods&ecomp=rzznk&earg=sr5&prid=ef50c0ae-9882-4e7b-b6fd-23b8257a21e8), dissenting).

Since Kotila was rendered, over two years ago, it has become increasingly clear that Justice Graves was correct in that requiring possession of all the chemicals or equipment to uphold a conviction under [KRS 218A.1432(1)(b)](https://advance-lexis-com.proxy.lib.umich.edu/document/?pdmfid=1516831&crid=849d3182-5ba6-4c04-afa9-d06b2d0290dd&pddocfullpath=%2Fshared%2Fdocument%2Fcases%2Furn%3AcontentItem%3A4JJ9-5VM0-TVV9-0200-00000-00&pdcontentcomponentid=7240&pdshepid=urn%3AcontentItem%3A7XW4-F4J1-2NSF-C3VF-00000-00&pdteaserkey=sr5&pditab=allpods&ecomp=rzznk&earg=sr5&prid=ef50c0ae-9882-4e7b-b6fd-23b8257a21e8) defies common sense. And though considerations of stare decisis would normally guide us to adhere to Kotila, we simply cannot overlook the fact that the Court's reasoning in subsequent decisions addressing [KRS 218A.1432(1)(b)](https://advance-lexis-com.proxy.lib.umich.edu/document/?pdmfid=1516831&crid=849d3182-5ba6-4c04-afa9-d06b2d0290dd&pddocfullpath=%2Fshared%2Fdocument%2Fcases%2Furn%3AcontentItem%3A4JJ9-5VM0-TVV9-0200-00000-00&pdcontentcomponentid=7240&pdshepid=urn%3AcontentItem%3A7XW4-F4J1-2NSF-C3VF-00000-00&pdteaserkey=sr5&pditab=allpods&ecomp=rzznk&earg=sr5&prid=ef50c0ae-9882-4e7b-b6fd-23b8257a21e8) has already departed significantly from the bright-line rule. Therefore, we go one step further and hold that HN2 Kotila's construction of KRS 218A.1432(1)(b) was incorrect.

[\*604] We do not reverse Kotila lightly. As the dissent observes in its extensive [\*\*9] discussion, HN3 stare decisis is an important guiding principle in American jurisprudence. On that point, we are in complete agreement. However, as this Court has noted recently, the doctrine of stare decisis does not commit us to the sanctification of ancient or relatively recent fallacy. While we recognize this Court should decide cases with a respect for precedent, this respect does not require blind imitation of the past or unquestioned acceptance ad infinitum. Rather, in many ways, respect for precedent demands proper reconsideration when we find sound legal reasons to question the correctness of our prior analysis.

## Cyber security

#### propaganda is cyber security concern

David M. J. Lazer, et al 2018, <https://itcs.ecu.edu/itcs-news/fake-news-misinformation-and-disinformation-as-cyber-security-threats/> \* “The Science of Fake News,” Science 09 Mar 2018: Vol. 359, Issue 6380, pp. 1094-1096.

In this edition of the IT Security Series, we discuss why misinformation and disinformation are emerging as cyber security threats, share approaches to help us become more critical news consumers, and provide fact-checking tools to determine when news content, images, and videos have been manipulated to deceive viewers. \* David M. J. Lazer, et al., “The Science of Fake News,” Science 09 Mar 2018: Vol. 359, Issue 6380, pp. 1094-1096. WHY ARE FAKE NEWS, MISINFORMATION, AND DISINFORMATION CYBER SECURITY THREATS? Fake news, misinformation, and disinformation have been a problem for some time; however, factors such as the continual increase in the frequency and sophistication of cyberattacks, election interference, and crises such as the COVID-19 “infodemic,” have made them a significant challenge for businesses, government agencies, financial markets, and the media.

## AT---T-Bowne

#### w/m – ptiv

#### C/I---Training and exercise programs are security coop

Fraser ’15 [Douglas; October 21; General (Retired), LLC, Former Commander of United States Southern Command; Statement of General Douglas M. Fraser before the House Armed Service Committee on Security Cooperation, https://www.hsdl.org/?view&did=789068]

Close Relationship Between Security Cooperation and Security Assistance Mr. Chairman, while this hearing is focused on security cooperation, from my experience, I think it is important to acknowledge the close relationship between Department of Defense security cooperation programs and Department of State security assistance programs. During my time in U.S. Pacific Command and U.S. Southern Command, both commands worked closely with the Department of State and the respective U.S. Embassies to coordinate security cooperation and security assistance programs. Training and exercise programs conducted through security cooperation meshed closely with the education and equipping programs conducted through security assistance programs. In fact, in many cases, more funding assistance to a country was provided through Department of State programs to enhance the capability of a nation’s armed forces, like Foreign Military Financing, than came from Department of Defense programs.

#### Their author agrees!

Bowne ’18 [Andrew; 2018; Major and Judge Advocate in the United States Air Force, Contract and Fiscal Law Professor, The Judge Advocate General's School, United States Army; Military Law Review, “Defending the New Fulda Gap: Deterring Russian Aggression Against the Baltic States Through Fiscal Legislation, 226 Mil. L. Rev. 147, lexis]

The lack of clarity for EDI authorities notwithstanding, efforts to build defense capacity in the Baltic States were bolstered by the overhaul of the security cooperation regime in the FY17 NDAA. In an attempt to simplify the quagmire that security cooperation authorities had become over the past fifteen years, Congress streamlined the dozens of various temporary and permanent sources of authority and codified them under one chapter in Title 10 of the U.S. Code. 125 Congress noted the increasingly more important role security cooperation plays in DoD operations, 126 and the below discussion of how EUCOM can leverage these new authorities to augment EDI demonstrates the potential utility such activities can have within NATO's deterrence strategy.

3. Defense Security Cooperation and the Baltic States

Since the terrorist attacks of 11 September 2001, Congress granted more authority to the DoD to engage in security cooperation with foreign militaries, a mission originally conducted by the DoS. Over that time, security cooperation became an integral part of the DoD's mission and is considered an important tool for executing its national security responsibilities. 127 The FY17 NDAA overhauled the previously unwieldy patchwork of authorities that made up the security cooperation regime and provides authority for the DoD to enhance interoperability and increase defense capability of friendly foreign militaries. As building partner capacity with newer NATO members is one of the five lines of effort under EDI, 128 these new authorities should be leveraged to the maximum extent possible by EUCOM in the Baltic States to ensure sufficient capability exists in that vulnerable region to deter Russia aggression. However, as discussed below, the source of funding for these authorities and whether they can be used in conjunction with EDI funds remains ambiguous.

a. Building Defense Capacity

Key among the changes is the replacement of 10 U.S.C. § 2282 on "Authority to Build the Capacity of Foreign Security Forces" with a new permanent authority that widens the scope of security cooperation the DoD can provide. 129 While the scope of Section 2282 was limited primarily to counterterrorism and stability operations, 130 broadens the scope of authorized foreign capacity building to include, among other purposes, training, and equipping for border security and operations or activities that contribute to an international coalition operation that is in the national interest of the United States. 131 Moreover, 10 U.S.C. § 333, Section 2282's replacement, will permit the DoD to provide lethal equipment on a global scale, which it was unable to do under Section 2282. 132 Finally, Section 333 allows the DoD to support the sustainment of previously provided equipment to foreign partners, whereas such sustainment was previously under the exclusive purview of the DoS through its Foreign Military Financing account. 133 This bureaucratic anachronism resulted in equipment at risk of disrepair, misuse, and inoperability by the foreign recipient. 134

Under the definitions section of the Security Cooperation chapter, security cooperation programs, such as those authorized by Section 333, include building and developing allied security capabilities for self-defense and building relationships that promote specific U.S. security interests. 135 The DoD should utilize these new authorities to build capacity in the security forces of the Baltic States in a way that it was unable to do so under the previous law. However, because Section 333 did not become law until the final days of Fiscal Year 2017 when it replaces Section 2282, 136 the utility of this new authority was largely unknown in FY17 and remains little used due to the complexity of funding Section 333 activities. Section 333 provides the sole source of funding shall come out of amounts authorized and appropriated for such fiscal year for O&M, Defense-wide, and available for the Defense Security Cooperation Agency. 137 However, Section 1241 of the FY17 NDAA adds additional sources of funding for Fiscal Year 2017 relevant to the Baltic States, including O&M Defense-wide, available for the Defense Security Cooperation Agency as specified in the funding table in Section 4301 of the FY17 NDAA, 138 as well as for the same line of items in the OCO O&M funding table in Section 4302. 139 The dual funding sources, O&M and OCO O&M, highlight the potential overlap between Section 333 capacity building, which are funded by O&M, and EDI capacity building, which is funded by OCO O&M. To avoid obligating funds from the wrong account, commanders must know whether the activity falls under EDI, and whether security cooperation funds can be used in addition to EDI or exclusively. Clarifying legislation can help resolve this confusion. 140

b. Operational Support to Foreign Forces

In addition to the replacement of Section 2282, the FY17 NDAA greatly expands the authority to provide support for conduct of operations to friendly foreign countries, replacing Section 1207 from the Fiscal Year 2016 NDAA, which was limited to providing support to African countries conducting counterterrorism activities. 141 Section 1245 of the FY17 NDAA, codified at 10 U.S.C. § 331, greatly expands the scope of the previous authority by eliminating geographic limitations. 142 This new authority provides funding of logistic support, supplies, and services to security forces in a friendly country, as well as small-scale construction projects to facilitate friendly country participation in U.S.-supported operations. 143

One provision that, if utilized by EUCOM, could meaningfully assist improving the defense capability in the Baltic States is the special procurement authority that allows the DoD to procure equipment "for the purpose of the loan of such equipment to the military forces of a friendly foreign country participating in a U.S.-supported coalition or combined operation." 144 This is "to enhance capabilities or to increase interoperability with [U.S. forces] and other coalition partners." 145 Because the intent of the authority is that the friendly country will reimburse the United States for the procurement, or the U.S. forces can to reuse the equipment, there is no limitation on the value of the procurement. 146

The DoD should utilize this authorization to procure an excess quantity of U.S.-used systems to ensure friendly forces use and train on the same equipment as U.S. forces. Use of equipment, coupled with training and exercises will increase familiarity and interoperability with U.S. forces and provide friendly foreign forces with confidence in operating weapon systems alongside the United States. A successful loan may influence the friendly force's procurement decisions, leading to more effective use of defense spending by the friendly force at no real cost to the United States, as the equipment is returned at the end of the loan period. However, it remains unclear as to what limitations on the type of procurement there are, if any. For example, the law is silent as to whether this section authorizes procurement for loaning weapon systems. 147 Nor does it provide the maximum duration of any loan. Nonetheless, the DoD should leverage the seemingly broad authority granted by Congress to procure equipment for the purpose of loaning such equipment to its allies to improve interoperability and bolster the defense capability of its allies in Eastern Europe.

c. Training and Exercises

Finally, perhaps the best way the DoD can maximize the operational readiness of its NATO partners is through extensive training and exercises. 148 Training of NATO members near Russia is essential to ensure those members, such as the Baltic States and Poland, can cope with hybrid warfare that may not trigger Article 5. 149 Moreover, frequent military exercises with U.S. forces can enhance those armed forces' capabilities. Wide-scale multinational exercises on NATO's eastern flank would also serve a dual purpose of reassuring allies and warning foes. 150 Recognizing the importance of multinational training and exercises, Congress sought to provide broader authority for commanders of combatant commands and service secretaries to authorize payment of certain expenses for friendly foreign countries resulting from participating in training and exercises with U.S. general forces. 151 This expands the previous authority, which was limited to payment of only incremental expenses to developing countries when authorized by the Secretary of Defense. This was only after a determination that "the participation by such country is necessary to the achievement of the fundamental objectives of the exercise and that those objectives cannot be achieved unless the United States provides the incremental expenses incurred by such country." 152 The new authority requires only the determination by the Secretary of Defense that support of the friendly foreign force is in the national security interest of the United States to do so, and expands the scope and type of payment for training and exercise expenses. 153 It allows a commander of a combatant command to authorize payment for expenses associated with training, exercises, deployment to such events, incremental expenses, and small-scale construction directly related to the effective accomplishment of such events, with the prior approval of the Secretary of Defense. 154

Beyond the benefit of paying for expenses to attract participation by other countries, this authority also appears to permit foreign forces to develop new capacity by allowing for training to improve the capacity of foreign forces beyond minimal level necessary to achieve interoperability, safety, or familiarization with U.S. forces in preparing for combined military operations." 155 While the new law states that the primary purpose of the training and exercises is to train U.S. forces, 156 there is no limiting language, such as restricting the training of foreign forces to only safety and interoperability. Thus, so long as U.S. forces are receiving the benefit of the training and exercises, the participation by other friendly forces and use of this authority for funding is permitted. Granting the DoD this authority allows it to better program more robust exercises and training focused on capacity building of the Baltic States' forces.

Consistent with the intent of EDI and RAP, EUCOM should use this authority to the fullest extent practicable to integrate multinational forces, particularly in command and control, intelligence, surveillance, reconnaissance, and cyber defense, where interoperability is critical to defending against Russian aggression. 157 Moreover, this authority's provision for small-scale construction permits to building necessary infrastructure within Eastern Europe that would otherwise be challenging for approval. Provided the project does not represent a foreign assistance program, structures built in support of U.S. military personnel participating in overseas training and exercises need not be temporary structures. 158 The explicit limitation on such military construction is that no one project may exceed $ 750,000 in costs, 159 and the implicit limitation comes from the absence of any authority for the maintenance of such construction projects after the completion of the exercise. Nonetheless, this authority appears to permit the United States to fund and build in a friendly foreign country, and the beneficiary can then decide to keep and maintain the project for its own future use. The resulting infrastructure will provide training and exercise opportunities where there may have been none absent this authority.

#### Prefer it.

#### A. OVERLIMITING. Banning wargaming and interoperability functionally limits the rez to just article 5 affs, which would auto-lose to “say no because every country has different systems”

#### A. PREDICTABILITY. It guides prep. Our ev is the gold standard---it’s from the House Armed Service Committee on Security Cooperation AND bowne concludes aff.

#### D. Functional limits check---Say no, EU and Unilat CPs, Ks, and other rez words.

#### E. Reasonability. Good is good enough.

## A5

#### . NATO isn’t just Article 5---Article 3 and 4 requirements require training and consultation, and cyber-attacks fall under non-Article 5 activities.

Brady ’13 [Colonel Brian H. Brady; October; Judge Advocate, U.S. Army assigned to the Defense Intelligence Agency Office of General Counsel Operations, former staff legal advisor (LEGAD) in the Office of the Legal Advisor, North Atlantic Treaty Organization (NATO), Allied Command Transformation, Joint Warfare Centre; 2013 Army Law. 4, “The North Atlantic Treaty Organization Legal Advisor: A Primer,” Department of the Army Pamphlet 27-50-485, lexis]

II. NATO Legal Authority

The North Atlantic Treaty Organization is a creation of international agreement. A mosaic of international agreements establishes the NATO Alliance, states its mission, and grants privileges and immunities to its subordinate elements. The next section provides an overview of some of these key agreements.

A. North Atlantic Treaty of 1949

The North Atlantic Treaty, also known as the Washington Treaty, establishes NATO legal authority, organization, and function. 11 NATO is both a political entity and a military entity. NATO's political leader is the Secretary General (currently Mr. Anders Fogh Rasmussen, a Danish citizen), while its military leader is the Supreme Allied Commander Europe (SACEUR) (currently U.S. Air Force General Philip M. Breedlove). The treaty establishes both a political and military role for the organization.

1. Core Mission and Article 5

Article 5 of the treaty states the core mission of NATO. 12 This mission is based upon article 51 of the UN Charter, which provides for collective self-defense. Article 5 states as follows:

The Parties agree that an armed attack against one or more of them in Europe or North America shall be considered an attack against them all and consequently they agree that, if such an armed attack occurs, each of them, in exercise of the right of individual or collective self-defense recognized by article 51 of the Charter of the United Nations, will assist the Party or Parties so attacked by taking forthwith, individually and in concert with the other Parties, such action as it deems necessary, including the use of armed force, to restore and maintain the security of the North Atlantic area. 13

NATO invoked the provisions of article 5 to the treaty for the first time in the aftermath of the 11 September 2001 attacks on the United States. 14 NATO Operation Active Endeavor (naval operations in support of 9/11 counterterrorism missions in the Mediterranean) was one of the first NATO operations authorized under article 5. 15

2. Non-Article 5 Activity

Not all NATO military activity can be justified under article 5 to the treaty. NATO member states 16 have an obligation to train and prepare for their defense. This is articulated in article 3 to the treaty. 17 The political aspect of NATO is reflected in the article 4 requirement that parties consult one another to resolve disputes or identify potential threats to the alliance. 18 These authorities have been interpreted to give NATO its own engagement activity (mirroring the activity of a U.S. combatant command), such as the Partnership for Peace and the Mediterranean Dialogue. 19 While article 5 is a good start point in articulating the legal basis for traditional NATO operations, the LEGAL) may also refer to underlying United Nations Security Council Resolutions (UNSCR) giving authority to engage in armed conflict under Chapter VII of the UN Charter. 20 In this light, NATO doctrine provides for operational responses beyond article 5 self-defense.

To address the multitude of security scenarios facing the alliance, NATO doctrine recognizes a category of activity known as Non-Article 5 Crisis Response Operations (NA5CRO). 21 Non-Article 5 operations cover contingencies that do not amount to a response to an armed attack on alliance territory. 22 The earliest example of this type of operation includes the NATO-lead of the Implementation Force (IFOR) in Bosnia-Herzegovina. 23 The doctrine states as follows:

## Coop

#### Cybersecurity is the protection and defense of both analogue and digital electronic devices and their communication channels---it can entail both defensive and offensive operations

RWCS ’20 [Real World Cyber Security; April 14; cyber analyst with deep expertise and extensive experience in embedded systems product development and product development security, including hardware security, secure boot, software and firmware security, network and protocol security, operating systems hardening, user interaction and user experience security, industrial design security, data protection and data privacy, cryptographic security, secure software development practices, security test and evaluation, government product security certifications and validation, intellectual property protection, import/export compliance, product liability, supply chain integrity, security in mergers and acquisitions, and corporate security governance; RWCS, “Defining Cybersecurity,” <https://medium.com/swlh/defining-cybersecurity-44cf1b1d6ae0>]

If You Can’t Properly Define Cybersecurity, How Can You Know What It Is?

It’s clear that the cybersecurity industry hasn’t been able to agree upon what cybersecurity is and isn’t. Even NIST, who is responsible for the definition of technical terms used by the U.S. Federal Government, has four different definitions of cybersecurity! At a minimum, there are dozens of different definitions of cybersecurity currently in use. Nearly all are incomplete in scope, some are horridly wrong, and nearly all fail to differentiate between cybersecurity and its information security cousin.

Background

If you look up the definition of “cybersecurity,” most of the answers you get are laughable. Most appear to be written by some “expert” with no actual concept of what cybersecurity is. Nearly all of those definitions sound as though they were written by an academic pontificating what he thinks cybersecurity theoretically should be, without himself ever having done any actual hands-on cybersecurity engineering.

Until July 2019, the sole “official” definition of cybersecurity (as defined by NIST) was: “The ability to protect or defend the use of cyberspace from cyber attacks.” Hyper-informative, wasn’t it? It’s about like telling a man who’s never seen a donut that, “A donut is a pastry shaped like a donut torus.” [See note 1.]

Then, just when you think it can’t get worse, it does. Now NIST can’t even agree within itself what cybersecurity is! It now four different definitions of cybersecurity! None of them tell you anything particularly useful about cybersecurity. Those definitions of cybersecurity are: [2]

Prevention of damage to, protection of, and restoration of computers, electronic communications systems, electronic communications services, wire communication, and electronic communication, including information contained therein, to ensure its availability, integrity, authentication, confidentiality, and nonrepudiation.

The ability to protect or defend the use of cyberspace from cyber attacks.

The process of protecting information by preventing, detecting, and responding to attacks.

The prevention of damage to, unauthorized use of, exploitation of, and — if needed — the restoration of electronic information and communications systems, and the information they contain, in order to strengthen the confidentiality, integrity and availability of these systems.

If you search online for a definition of cybersecurity, most definitions are just as bad — if not worse — than the definitions NIST provides. Here are some examples:

Measures taken to protect a computer or computer system (as on the Internet) against unauthorized access or attack. [3]

The art of protecting networks, devices, and data from unauthorized access or criminal use and the practice of ensuring confidentiality, integrity, and availability of information. [4]

May also be referred to as information technology security. [5]

The preventative techniques used to protect the integrity of networks, programs and data from attack, damage, or unauthorized access. [6]

The practice of protecting systems, networks, and programs from digital attacks. [7]

The protection of information assets by addressing threats to information processed, stored, and transported by internetworked information systems. [14]

Notice the pattern? The definitions all talk about defending computers, networks, and data. That isn’t what cybersecurity is. That’s what information security is! Plus, the scope is strictly digital in many cases. Clearly, whoever wrote those definitions have no experience with industrial controls security, where even analogue devices can be at risk of attack. [8]

We have two problems here. First, we have failed to define what cybersecurity adequately or accurately is. Worse, we are trying to somehow shoehorn cybersecurity into being either the same as information security or some subset of information security. It isn’t, and I’ll go into detail why in a minute.

So, if we can’t even agree upon what cybersecurity is, how can we possibly expect to create reasonably secure systems and products that depend upon an in-depth understanding of cybersecurity?

Clearly, we can’t.

And, the problem is compounded by the mindset that the same tools and techniques used for information security are applicable to cybersecurity. Yes, most information security tools and techniques can be applied to cybersecurity, but cybersecurity requires tools and techniques which go far beyond those of information security.

How can we expect to secure our systems when we are using the wrong tools? Or, at best, an incomplete set of tools?

Again, clearly, we can’t.

In my professional opinion, the root of the problem we’re facing is that too many “cybersecurity experts” began their careers as “information security experts” and never have had actual hands-on cybersecurity experience beyond applying partial aspects of cybersecurity to information systems. Thus, we are left with information-centric definitions of cybersecurity, where the “experts” have tried to mold cybersecurity into the shape of information security.

Well, it’s time to break that mold!

Let’s get started with a few definitions.

Definitions

First, let’s define security:

Security is the protection of assets from threats.

That’s fairly clear, but let’s dissect it to ensure the subtleties are covered:

Assets are anything tangible or intangible that has value. In the context of security, usage of the word “asset” usually refers to a “protected asset.”

Protected Assets are any asset protected by a security service. Examples of protected assets could include: data or information (electronic or physical), network and computing infrastructure, software, products and associated intellectual property, people (employees, customers, vendors), real estate and personal property, and utilities and other critical infrastructure. That is, anything of value is a potential protected asset.

Security Services are any threat reduction capability provided by security. There are five generally recognized security services: Confidentiality, Integrity, Availability, Authenticity, and Access-Control. (See the blog post, What Are The Fundamental Services Provided By Security? Hint: CIA Is Not The Answer for additional details.)

Threats are anything with the potential to cause harm. For example, the potential for an attack to occur. Threats can be either intentional (e.g., sabotage) or accidental (e.g., aircraft bird strike), and they can be both man-made events (e.g., human errors, cyber attacks, power failures, and network outages) or natural events (e.g., fires, floods, earthquakes, hurricanes, and tornados). Also, see security threats, below.

Attacks are any action taken against an asset with the intention of causing harm.

Security Threats are anything that may cause harm to a protected asset and/or associated entities. For example, whereas a security threat that discloses personally identifiable information would most likely inflict minimal harm to the asset that held the disclosed information, the disclosure itself could do considerable harm to both the organization’s brand and to the individuals whose information was disclosed. There are seven generally recognized categories of security threats: Denial of Access, Forgery, Spoofing, Repudiation, Unauthorized Access, Unauthorized Disclosure, and Unauthorized Modification (see blog post referenced in Security Services for more details.).

Entities, in the context of security, are anything that attempts to use a protected asset. An entity can be a person, software, robot, or anything else that attempts to use a protected asset.

Okay, I lied: That definition has a lot of subtly buried within it. Hopefully, now the definition of security has a deeper meaning for you.

So, that’s the definition of the mission of security across all of the organization’s security domains. In most organizations, there should be three top-level security domains:

Corporate Security

Information Security

Cyber Security

Now, let’s define each of those security domains.

Corporate Security

Corporate Security is those aspects of an organization’s security not directly related to technology.

That is, in general, corporate security is those aspects of security that pre-date technology or technological security solutions, or are unrelated to technology. Falling under the corporate security domain would be aspects of security related to employee services, safety, environmental services, or facilities; or which are intellectual property, legal, or regulatory in nature. (This is not an all-inclusive list.)

In other words, much of what you would think of as an organization’s security before the advent of digital technologies falls into the corporate security domain.

Today, corporate security often makes extensive use of technology. But, corporate security’s technology is often not under the auspices of information security or cybersecurity. Without close collaboration between security groups, serious gaps in security defenses will occur.

Worse, there often isn’t a corporate security group in the organization. Instead, you often find aspects of corporate security disbursed between multiple (and, often non-communicating) groups, such as human resources, facilities, safety, plant protection, legal, risk management, and environmental.

I plan to discuss corporate security in more detail in an upcoming blog post, Corporate Security: The Forgotten Security Domain.

Information Security

Information Security is the protection of information in any form and at all times.

That’s pretty much the classic paragraph-long definition of information security, summarized into one sentence.

Now, let’s dissect it to get a deeper understanding of what that means.

Security is the protection of assets from threats.

Protection is the rendering safe from harm. Protection is passive security. That is, security that does not offer a response to an attack. It is equivalent to putting a lock on a door to secure your house.

In any form means it includes both physical (e.g., printed documents) and electronic (e.g., files and databases) information.

At all times means the information must be protected, whether it is at rest (i.e., in storage), in use, or in motion (e.g., electronic information sent over a network, or a printed document transported by a courier).

Thus, we define information security as the protection of information. Note that we didn’t place any constraints upon the scope of protection. That is, if we have to protect computers and networks to protect information, then that would be within the scope of information security. But, keep in mind that the objective is the protection of information. Nothing more. Nothing less.

Cyber Security

We’ve already shown that there isn’t a commonly agreed-to definition for cybersecurity. Now, I’m going to propose a definition for cybersecurity which covers all aspects of cybersecurity — something which is lacking from other definitions — while providing a clear distinction from information security. [10]

Cybersecurity is the protection and defense of both analogue and digital electronic devices, their communications channels, and their processing-and-control logic and algorithms.

Now, let’s dissect that definition to get a deeper understanding of what it means and its ramifications.

Security is the protection of assets from threats.

Protection is the rendering safe from harm. Protection is passive security. That is, security that does not offer a response to an attack. It is equivalent to putting a lock on a door to secure your house.

Defense is an action taken to resist an attack. Defense is active security. This means that you have dynamic security with ever-changing defenses — which can include offensive actions to stop an attack. It is the equivalent of confronting an intruder in your house with a loaded weapon.

Digital Devices are any electronic device that uses discrete data and processes for all its operations. This clearly includes computers, cell phones and tablets, routers, switches, WiFi access points, and firewalls, but it also includes all other digitally networked devices, such as all IoT devices, VoIP telephones, digital security cameras, smart badge readers, etc.

Analogue Devices are any electronic device that uses continuous data and processes for all its operations. This would include landline telephones, fax machines, most nuclear reactor control systems, older radar systems, older industrial controls, some satellite and other space systems controls, and literally thousands of other devices. In industrial controls situations, analogue devices often serve as failsafe backups to digital controls.

Communications Channels are the means by which a device is connected to other devices. For analogue device communications, this could be a simple wire or wire-pair, coax cable, analogue radio, or similar technologies. For digital device communications, it would include any type of wired or wireless network. For digital to analogue device communications, it could include any of the previously mentioned means of analogue device communications used to communicate to an analogue interface in the digital device.

Processing Logic and Algorithms are the means by which a device accomplishes its designated purpose. For analogue devices, this is all done in hardware. For digital devices, this includes both hardware and software (microcode, firmware, operating systems, applications, etc.).

Control Logic and Algorithms are the means by which a device regulates its processing. For analogue devices, this is all done in hardware. For digital devices, this includes both hardware and software (microcode, firmware, operating systems, applications, etc.).

Now, let’s put the phrases together and detail the bigger picture.

Is the protection and defense is cybersecurity’s first significant difference from information security. Cybersecurity not only offers protection like information security, but it also offers defense. In other words, cybersecurity can take the offensive actions necessary to defend systems.

Of both analogue and digital electronic devices is the next significant difference from information security, as information security’s tools seldom address analogue devices. It is also different in that information security offers protection of non-electronic information (e.g., printed), whereas cybersecurity only deals with electronic devices and their data. [11]

This definition means that protection and defense are also offered to the electronic devices (components) combined to construct a more complex electronic device. For example, protection and defense would be offered to CPUs, GPU, FPGAs, ASICs, NICs, DACs, memory, controllers, and all the other various analogue and digital components that comprise a modern end-purpose electronic device, such as a smartphone or a computer. In other words, cybersecurity protects and defends any security-sensitive electronic device, be it analogue or digital, and be it an end-purpose device or a component of such a device.

Their communications channels is again a difference between cybersecurity and information security. Cybersecurity provides both protection and defense of the electronic communications channels themselves, both analogue and digital. Whereas, information security only provides for the protection of the information conveyed over those communications channels.

Additionally, information security also provides for the protection of information communicated by non-electronic means (e.g., printed documents), which is outside the scope of cybersecurity.

And their processing-and-control logic and algorithms is the final difference between cybersecurity and information security. Cybersecurity offers protections to both hardware and software, and can take actions to defend both from attack. By contrast, information security only provides passive protection to information.

So, that is the definition of cybersecurity and an explanation of its scope.

To recap, cybersecurity provides security for all electronic technology, except for the information processed by such technology (information is protected by information security).

Or, another way to view the difference between information security and cybersecurity is that information security secures the information itself, and cybersecurity secures everything that creates, uses, processes, stores, or communicates that information.

Where Information Security Fails Us

In my blog introduction, I state that “trying to treat cybersecurity problems as though they are information security problems” is one of the fundamental mistakes we are making in security today. The lack of an understanding of the differences between information security and cybersecurity is the root cause of this problem.

As we have seen in the preceding definitions, information security is “data-centric,” and cybersecurity is “device-centric.” Trying to apply information security principals to “device security” creates two problems: First, you can’t adequately secure “hardware” using the same controls used to secure data; And second, there is nothing in information security that provides for an active defense.

Let’s look at some of the issues that the premises supporting information security fail to address. To do this, we’ll examine an example from product security.

The overwhelming insecurity of IoT products has filled the news recently. Why? Many would say that it’s a simple matter of companies trying to produce products on the cheap. However, I would argue that the issue is more likely the product’s designers’ failure to recognize the potential for security problems in their products.

I believe that fundamentally, such product failures are compounded by an incomplete view of security: a view driven by an information security focus. A focus that, for embedded systems products (such as IoT devices), is incomplete, at best. Why incomplete? Because most security issues with IoT devices are not information related. Rather the problems are with the devices themselves.

Let’s begin by listing some of the security questions that product designers should be asking, but are obviously not asking. And, with most product security practitioners coming from an information security background, those product security architects probably do not even know they should be asking these questions.

After all, why should they know better? Nothing they had learned in the scope of information security would indicate that these are issues with which to be concerned. The types of product security questions (that is, cybersecurity questions) which all product security architects should be asking include:

How do you prevent reverse engineering of the product?

How do you prevent tampering with the product?

How do you prevent the production of unlicensed clones of the product?

How do you prevent access to the hardware interfaces used for development debugging of the product?

How do you prevent access to the hardware interfaces used for manufacturing testing of the product?

How do you perform failsafe firmware updates of the product (such that a failed update does not brick the product)?

How do you prevent unauthorized modification of the product’s firmware?

How do you prevent your firmware from running on third-party devices?

How do you ensure the integrity of your supply chain?

How do you prevent unauthorized modification of the device itself?

How do you prevent misuse of the device from damaging the device itself (e.g., using a USB port on a device for other than its intended purpose, and drawing too much power)?

How do you prevent misuse of the device from creating a safety incident (e.g., using an aerosol can to create a vapor fog to trigger a motion detector to unlock a door)?

How can this device be abused by an attacker to cause harm?

How can we verify that our UI is always unambiguous to its intended audience?

How can we verify that our UX is always intuitive to its intended audience?

How can we verify that our UI creates neither security or safety issues?

How can we verify that our ID creates neither security or safety issues?

And this is just a very small sample of the questions that every product development organization should be asking, but which is clearly failing to occur.

Now, I can already hear the objections: “These are hardware engineering issues, not information security issues, and that’s why they’re not covered by information security.” Well, that’s half wrong and half right. Wrong, in that they are not hardware engineering issues; rather, they are hardware security issues. Right, in that they are not information security issues; rather, they are cybersecurity issues. [12]

These, and tens of thousands of other similar issues, are being left unaddressed during product development because information security doesn’t address these types of issues. Nor should it, as those issues are cybersecurity issues and not information security issues.

Nothing in an information security professional’s background or training would prepare them to even know that they should be asking the types of questions I posited. And, that’s what should be expected, because these are not information security issues and I would not expect an information security professional even to have half-a-clue that such problems exist. It’s for precisely this reason that cybersecurity exists and is different from information security.

The problem is really simple: Information security exists to protect information. Nothing in the fundamentals of information security was ever intended to secure anything other than information. Thus, we need to stop trying to use an information security mindset to secure “stuff” that isn’t information. We must recognize that cybersecurity’s scope is beyond that of information security, and thus apply cybersecurity principals to cybersecurity problems.

Defense

We also need to remember that cybersecurity allows for active measures to defend devices. There’s a reason that the military and intelligence agencies refer to their security operations as cybersecurity, and that’s because they take active countermeasures to attacks. You don’t do that when your objective is to secure information. In fact, that entire concept is an anathema to the information security principals and mindset.

Cybersecurity defense is a big rabbit hole I don’t plan to explore further in this posting, other than to remind you that cybersecurity’s objective is the protection and defense of assets.

Summary

There is an old saying, “When the only tool you have is a hammer, everything looks like a nail.” With no real cybersecurity experience, too many information security experts are trying to hammer cybersecurity into becoming an information security nail. We need to reset the thinking of those information security professionals and teach them that cybersecurity is more like a bolt than a nail, and that you use a wrench, not a hammer, when installing or removing a bolt.

Now, a quick review…

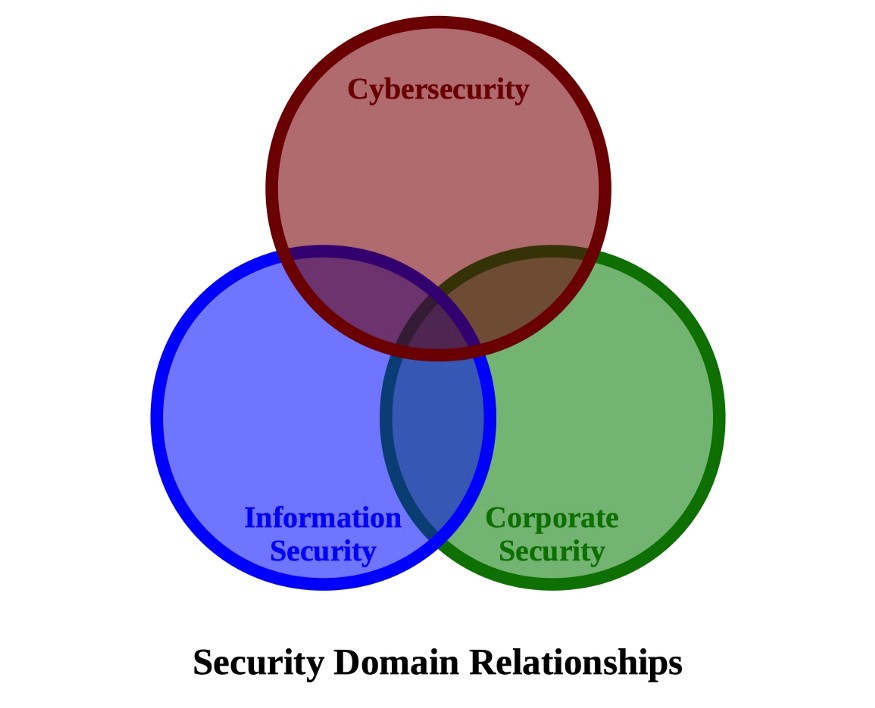
In most organizations, there are three security domains with which it must be concerned:

Corporate Security, which protects (and sometimes defends) people; and real, corporate, and intellectual property.

Information Security, which protects information (data).

Cybersecurity, which protects and defends: hardware, communications, and software.

The diagram below illustrates those relationships among the organization’s security domains.



We established the following definitions in support of those security domains:

Security is the protection of assets from threats.

Corporate Security is those aspects of an organization’s security not directly related to technology.

Information Security is the protection of information in any form and at all times.

Cybersecurity is the protection and defense of both analogue and digital electronic devices, their communications channels, and their processing-and-control logic and algorithms.

Trying to treat cybersecurity problems as though they are information security problems is one of the fundamental mistakes we are making in security today. We have to remember that information security is “data-centric,” and cybersecurity is “device-centric.” Trying to apply information security principals to “device security” creates two problems:

You cannot adequately secure “hardware” using the same controls used to secure data, and

There is nothing in information security that provides for active defense.

If you search the Internet, you will find that many so-called “information security experts” claim that cybersecurity is a subset of information security. But, compared to information security, cybersecurity has a substantially broader scope, addresses a more complex set of security threats, and offers active defenses not provided by information security.

If anything, we should view information security as a subset of cybersecurity. However, that’s not accurate either, as what those two domains are attempting to secure is different — data vs. hardware, software, and communications. Some overlap between the two is unavoidable, but at the most fundamental levels, they are attempting to solve different problems. [13]

Thus, we need clear, concise, unambiguous definitions of both cybersecurity and information security.

Hopefully, you will find the definitions provided here meet those criteria.

So, don’t let alleged information security experts try to tell you what is and is not cybersecurity! Those so-called “information security experts” are precisely that, and nothing more, because they clearly do not understand cybersecurity!

Please leave cybersecurity to actual cybersecurity practitioners.

Thank you!

#### General terms like “security cooperation” should be understood broadly.

Scalia ’12 [Antonin Scalia and Bryan Garner; 2012; Justice on the Supreme Court of the United States; American lawyer, lexicographer, and teacher; Reading Law: The Interpretation of Legal Texts, “General-Terms Canon,” Ch. 9]

General terms are to be given their general meaning (generalia verba sunt generaliter intelligenda).

Without some indication to the contrary, general words (like all words, general or not) are to be accorded their full and fair scope. They are not to be arbitrarily limited. This is the general-terms canon, which is based on the reality that it is possible and useful to formulate categories (e.g., “dangerous weapons”) without knowing all the items that may fit—or may later, once invented, come to fit—within those categories.