# \*\*Neg\*\*

# Cyber Advantage

### 1NC---No Retal

#### NATO can’t retal!

Rowland Manthorpe 22 [Rowland Manthorpe, 6-28-2022, "Could the Russian cyber attack on Lithuania draw a military response from NATO?", Sky News, https://news.sky.com/story/could-the-russian-cyber-attack-on-lithuania-draw-a-military-response-from-nato-12641986, DOA: 7-18-2022 //ArchanSen]

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. Less worrying than we are often led to believe Cyber attacks aren't like physical attacks, where the size of the damage roughly corresponds to the size of the assault. Online, being "massive" doesn't really mean that much. Ditto "intense", another word used to describe the attack. This is one reason why, for all the frightening rhetoric that surrounds them, many experts believe that cyber attacks are generally much less worrying than we are often led to believe.

### Cyber---No Nuke War

#### No nuclear escalation. They don’t benefit from it.

Lanoszka 19 [Alexander Lanoszka, Assistant Professor of International Relations at the University of Waterloo. Previously, he taught at City, University of London and has held fellowships at the Massachusetts Institute of Technology and Dartmouth College. His research on alliance politics, theories of war, and European security has appeared in International Security, Security Studies, International Affairs, Survival, and other academic journals. He holds a PhD from Princeton University; 8-21-2019; "Nuclear Blackmail and Nuclear Balance in the Baltic Region"; No Publication; https://sjms.nu/articles/10.31374/sjms.22/; KL]

Would Nuclear Coercion Be Effective Against the Baltic Countries and NATO?

Russian attempts at nuclear blackmail will likely be ineffective. First, as many analysts point out, Russia does not need to use nuclear weapons in order to conquer the Baltics. The force ratios already heavily favor it, even with NATO’s enhanced Forward Presence being regionally deployed since 2017 (Lanoszka & Hunzeker 2019; Shlapak & Johnson 2016). Second, threats to use nuclear weapons lack believability. Not only would it deepen Russia’s isolated international status, it would also most likely precipitate the very thing that Russia would prefer to avoid: greater involvement by the United States. Why would it risk its own complete destruction for the sake of taking three Baltic countries, especially when Kaliningrad already gives it access to the Baltic Sea? Third, a sudden move against the Baltic countries would be offensive in nature. It would not involve Russia having its back up against the wall. If the United States were to attack Russia, then nuclear weapons use could be expected. As stated earlier, Russia would be peculiar if it allowed hostile forces to attack it successfully using conventional military weapons.

#### MAD.

Lanoszka 19 [Alexander Lanoszka, Assistant Professor of International Relations at the University of Waterloo. Previously, he taught at City, University of London and has held fellowships at the Massachusetts Institute of Technology and Dartmouth College. His research on alliance politics, theories of war, and European security has appeared in International Security, Security Studies, International Affairs, Survival, and other academic journals. He holds a PhD from Princeton University; 8-21-2019; "Nuclear Blackmail and Nuclear Balance in the Baltic Region"; No Publication; https://sjms.nu/articles/10.31374/sjms.22/; KL]

Implications for Baltic Security

Given these parameters of the security environment in the Baltic region, what are the prospects of nuclear coercion? Recall the three points made earlier. First, escaping MAD is extremely difficult and costly. Even when the United States enjoyed nuclear superiority over the Soviet Union, its leaders did not believe that they were invulnerable to a devastating riposte. Second, leaders might still think that they can leverage coercive advantages from their nuclear weapons. Third, despite these beliefs, nuclear coercion does not have a good track record, with its effectiveness highest when the circumstances are defensive and extreme.

Can Russia Escape MAD?

Russia would face tremendous hurdles if it were to try to overcome MAD. To do so, its current modernization program would be inadequate since it would need to launch a bolt-from-the-blue first strike against all three legs of the U.S. nuclear triad. Specifically, Russia would have to enhance its submarine warfare capabilities significantly in order to track and to kill American (and British) nuclear-powered ballistic missile submarines that could launch SLBMs against Russian targets. It would need capabilities for destroying hardened ICBM sites located across the United States and striking airbases before nuclear-armed bombers can take off. It would also need to develop a sophisticated air defense system to destroy any incoming long-range, stand-off nuclear missiles that the United States is hoping to get for those bombers. In a strategic exchange, Russia must achieve all of these tasks before U.S. nuclear weapons rain down on Russian cities and military sites. Since the 1970s at least, the United States has been developing impressive counterforce capabilities due to improvements in remote sensing, guidance systems, data processing, communication, and other computing technologies (Lieber & Press 2017: 18–32). That Britain and France have their own nuclear arsenals also complicates Russian targeting.

Escaping MAD does not appear to be a goal behind the motivation of Russia’s modernization program (Podvig 2018). To the contrary, Russian military strategists are acutely aware of their country’s inferiority relative to the United States and NATO. As chief of the General Staff, Marshal Nikolai Ogarkov recognized in the early 1980s that a revolution in military affairs was afoot. Conventional weapons gained effectiveness thanks to advances in guidance systems and information processing. He and his colleagues began to appreciate that Warsaw Pact forces could soon lose their long-held advantages with regard to the conventional balance (Adamsky 2010: 28–32). The Cold War ended within a decade and Russia oversaw the rapid deterioration of its armed forces throughout the 1990s. The modernization programs overseen by Putin and his defense ministers have served to rectify the neglect during those years (Renz 2016). Nevertheless, Russian military theorists write extensively of the unfavorable strategic balance. Retired General Makhmut Gareev (2016), current Chief of the General Staff Valery Gerasimov (2014), S. G. Chekinov, and S. A. Bogdanov (2011), and current Commander of the Western Military District A. V. Kartapolov (2015) have all opined how Russia has lagged behind the United States and the West in its ability to fight non-traditional wars – that is, wars in which information and proxy conflicts play major roles.

### Cyber---No Baltics War

#### No Baltic war.

SIAS 22 [Dragonfly's Security Intelligence & Analysis Service (SIAS); 3-28-2022; "Baltics"; Dragonfly Intelligence; https://www.dragonflyintelligence.com/news/baltics-impacts-of-ukraine-conflict/; KL]

In particular, they have asked us what the likelihood is of Russia invading Estonia, Latvia or Lithuania, and to a lesser degree what the likely knock-on effects are on these countries from a prolonged conflict in Ukraine.

Our top line forecasts for the Baltic states are as follows:

* It is highly unlikely that Russia will initiate an invasion of any of the Baltic states in coming months, particularly while its military is engaged in Ukraine.
* At more than 300km at their closest, it is very unlikely that the fighting in Ukraine will lead to any inadvertent military escalation or accident in the Baltic states.
* There is a reasonable chance of a military accident in countries directly bordering Ukraine involving NATO and Russian forces, but we anticipate that both would seek to de-escalate quickly in this event.
* In the longer term, citizens in the Baltics are highly likely to feel the brunt of Western sanctions and Russia’s economic retaliation, with high gas prices and drops in trade volume directly impacting businesses and households.

#### Zero means or motive.

SIAS 22 [Dragonfly's Security Intelligence & Analysis Service (SIAS); 3-28-2022; "Baltics"; Dragonfly Intelligence; https://www.dragonflyintelligence.com/news/baltics-impacts-of-ukraine-conflict/; KL]

Military implications

Our interstate conflict risk ratings for the Baltic states are low. All three are NATO members, and so the rest of the alliance are bound to them by Article 5 on collective defence. Russia has shown little to no aggressive intent or presented any kind of genuine military threat towards the Baltics in recent years, nor since the invasion of Ukraine. And with a significant proportion of its forces now inside Ukraine (and sustaining major casualties), Russia probably lacks the resources to commit an invasion-scale force to the Baltics, at least any time soon.

#### No chance of accidents.

SIAS 22 [Dragonfly's Security Intelligence & Analysis Service (SIAS); 3-28-2022; "Baltics"; Dragonfly Intelligence; https://www.dragonflyintelligence.com/news/baltics-impacts-of-ukraine-conflict/; KL]

The proximity of Russian airstrikes and anti-aircraft fire to Ukraine’s borders with Hungary, Poland, Romania and Slovakia (all NATO members) means there is a risk of a military accident there, albeit a low one. Our three main scenarios for such an event include a Russian military aircraft violating NATO airspace, Russia striking a NATO country-flagged vessel in the Black Sea, and Russian projectiles fired in Ukraine landing in NATO territory (see P-14-03-22-EU/EA-1 for a detailed breakdown of these scenarios).

Of these, a Russian aircraft crossing into NATO airspace is the most likely to affect the Baltic states. Russian jets often made such incursions prior to the conflict, prompting NATO to start the Baltic Air Policing initiative in 2004. We have not seen reports of any incursion there since the invasion. But even if such an incident happened, we anticipate that their militaries would refrain from shooting a Russian aircraft down and only scramble their jets to escort it away. This is what Hungary did when an unidentified military drone from Ukraine crossed its airspace on 10 March.

Even if any of these scenarios occurred, we still anticipate NATO and Russia would very probably try to prevent tensions from escalating into a wider conflict. But it is likely that NATO would deploy more forces on its eastern flank and member states in the region adopt some emergency measures, with potential operational impacts for organisations based there. In the absence of precedent, we assess that this would plausibly range from military deployments temporarily disrupting operations at airports, increased checks on goods and people on the borders, up to national states of emergency and closures of airspace.

#### Russia won’t use ethnic justifications.

SIAS 22 [Dragonfly's Security Intelligence & Analysis Service (SIAS); 3-28-2022; "Baltics"; Dragonfly Intelligence; https://www.dragonflyintelligence.com/news/baltics-impacts-of-ukraine-conflict/; KL]

One outlier scenario that clients have raised with us relates to Moscow alleging violations of the rights of ethnic Russians in the Baltics to justify a military intervention. This is what it did ahead of the invasion of Ukraine in February, as well as in Crimea in 2014. Russian speakers account for around 34% of the population in Latvia, 30% in Estonia, and 8% in Lithuania. But we assess that this scenario is extremely unlikely at this stage. Russia’s influence over Russian ethnic minorities in the Baltics has declined in recent years, particularly after the authorities shut several Russian-language media outlets after 2014.

# Modeling Advantage

## SQ Solves

#### SQ Solves

Ministry of Energy of the Republic of Lithuania 2021 (06/18/2021, “Baltic energy security issues at the centre of US attention” https://enmin.lrv.lt/en/news/baltic-energy-security-issues-at-the-centre-of-us-attention)

“Strengthening energy sector cybersecurity preparedness remains a national security priority for all countries,” said Vice-Minister of Energy Albinas Zananavičius at the second meeting of the transatlantic high-level working group that took place on 15-17 June in Washington, DC (USA). According to Mr Zananavičius, the need to focus efforts on strengthening competencies in this area is confirmed by the still frequent cases of attacks by hostile countries against national energy infrastructure. This working group for strengthening cooperation between the United States and European countries in the field of energy cybersecurity was established during the second meeting of the Partnership for Transatlantic Energy Cooperation (P-TEC) that was held in Vilnius in 2019. The working group is chaired by Lithuania and the United States, and other member nations – Estonia, Latvia, Poland, Bulgaria and Croatia – participate in its activities. “Cyber-attacks on energy infrastructure are a cross-border threat. They pose equally serious concern about the security of our energy infrastructure on both sides of the Atlantic. Therefore, we must work together by sharing both good practices and lessons learned in this area,” said Mr Zananavičius, inviting the countries participating in the working group to continue the work started. One example of a cyber-threat is the attack on a top US fuel supplier a month ago. Progress in implementing the working group’s action plan was also discussed during the meeting. The countries mutually agreed that the Cyber Strike Workshop held by experts from the US Department of Energy’s Idaho National Laboratory this March-April was very useful in strengthening the cyber security competencies of experts working in the energy sector. This is one of the first examples of successful collaboration in this format. The members of the working group agreed to continue their cooperation in implementing the objectives set out in the action plan. For example, one of the most important goals for Lithuania and the other Baltic States is to strengthen cyber security capabilities for their synchronisation with the continental European network. During the visit, Mr Zananavičius also met with representatives of the US Administration, Department of Energy, State Department and Congress, as well as with energy companies operating in the field of liquefied natural gas and green energy technologies such as hydrogen. During the meetings, the Vice-Minister of Energy presented the energy security situation in the region and Lithuania’s goals in strengthening energy independence and security. US representatives reaffirmed their support for Lithuania in pursuing greater energy independence and energy security. The US will continue to support energy security issues in Europe that require special attention, including natural gas diversification and Nord Stream 2, as well as nuclear safety in the EU neighbourhood.

## No modeling

#### Rehighlighting ---- No modeling, their ev says so

Dana 7-12 (Joseph, Joseph Dana is the former senior editor of Exponential View, a weekly newsletter about technology and its impact on society. He was also the editor-in-chief of emerge85, a lab exploring change in emerging markets and its global impact. Masters in European History/Jewish Philosophy @ Central European University. “Cyberattacks in Baltics foreshadow future of war”, https://asiatimes.com/2022/07/cyberattacks-in-baltics-foreshadow-future-of-war/)LR

As the fighting in Ukraine drags on, another conflict is taking shape elsewhere on Russia’s periphery. This borderless conflict is aimed at destabilizing the Baltic states of Estonia, Latvia and Lithuania, but can and likely will expand to engulf others. Last month, Lithuanian government and public service Web portals were hit by a sustained cyberattack from Russian hackers. The attack was a response to Lithuanian enforcement of a European Union sanctions package on goods traveling to and from Kaliningrad, a Russian territory located between Lithuania and Poland. In taking responsibility for the attack, Russian hackers promised that more would be forthcoming. “The attack will continue until Lithuania lifts the blockade,” a spokesman for the group told Reuters. “We have demolished 1,652 Web resources. And that’s just so far.” The Baltic states have been on the front lines of cyber warfare for decades. As the first countries to establish independence from the Soviet Union in the early 1990s, they have remained decidedly anti-Russian in their posture and thus have borne the brunt of Russia’s increasingly sophisticated cyber offensive. In 2007, the Estonian parliament, several ministries, media institutions, and banks suffered a series of severe cyberattacks over the country’s stance on relocating a Soviet-era monument in the capital Tallinn. Officials in the Baltics viewed the attack as a precursor to an offensive that could knock out power grids and make the country in essence ungovernable. The severity of the offensive, which lasted 22 days, forced Estonia to set up measures to insulate the country from digital warfare. The approach was simple: Put as many government services and systems on private, secure networks and beef up cybersecurity. Such a model wouldn’t work in every country. Still, given their small sizes and large information-technology sectors, the Baltic states offer a blueprint for how cybersecurity systems can be built to withstand the vulnerabilities of our technological age. The silver lining of this defensive posture is that Baltic citizens live in digital republics, as The New Yorker once described Estonia. By investing in complex digital infrastructure, the Estonian government enables citizens and residents to conduct most of their lives online. They can sign and access virtually all government services digitally using their unique Estonian digital identity, a system that was established in 2002. 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. 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.

# EU

### EU-NATO P3 CP---1NC

#### EU-NATO-P3 solvency advocate

Lété and Pernik 17. Bruno Lété is a senior fellow for Security and Defense Policy in the Brussels office of The German Marshall Fund of the United States. Piret Pernik is a research fellow at the International Centre for Defence and Security in Tallinn; “EU–NATO Cybersecurity and Defense Cooperation: From Common Threats to Common Solutions”; December 2017; GMF; <https://www.gmfus.org/sites/default/files/EU-NATO%2520Cybersecurity%2520and%2520Defense%2520Cooperation%2520edit.pdf> //BY

Getting Ahead of the Evolving Threat The task now for the EU and NATO is to find consensus around how to approach and limit cybersecurity threats. Transatlantic cooperation is key to more effectively prevent, detect, and deter cyber-attacks, as well as to hold the perpetrators accountable. As such, the EU and NATO must continue to think how to deepen and widen existing cooperation in cybersecurity and defense. The following recommendations are not necessarily implementable tomorrow, but they are achievable. We offer some ambitious goals to work toward, envisioning what the EU and NATO “should” do, not only what they “can” do, within current political realities. Develop a Joint Cyber Threat Analysis Hub The European Union and NATO have already demonstrated their ability to work together in jointstructures, most recently through their support for the European Centre of Excellence for Countering Hybrid Threats in Helsinki. Creating an EU–NATO Cyber Threat Analysis Hub could be another significant step toward institutional cooperation. The first task of the Hub would be to monitor and analyze technical level early-warning indicators on cyber threats and provide enriched output for operational and strategic levels. The Hub would leverage capacities provided by relevant EU and NATO institutions, as well as the private sector. Clearly, it will not be easy to bring these actors together. Nonetheless, this structure would be the ideal for building a shared civilian-military, public-private, and EU– NATO situational awareness. Such a hub would bring together all-source information (open-source, anonymized, and sanitized information from public and non-public sources, including classified ones), and analyze it to foster shared situational awareness. Operational level incident situation reports from EU and NATO entities should be shared in the Hub, and it would have a central role in sharing strategic level reports in case crisis response mechanisms are activated by the EU or NATO. The Hub should act to improve information sharing, by developing technical and operational level Standard Operating Procedures (SOP) for information exchange between the EU and NATO entities. The Hub could also facilitate both informal ad hoc and formal regular information sharing and enable secure lines of communication to share confidential cyber intelligence. As a first trust-building measure for better information sharing, the Hub could therefore help define what type of information needs to be shared, who needs to receive it, when the information needs to be shared, and make sure the information is released in a timely and appropriate manner. An G|M|F December 2017 4 Policy Brief important function in this respect would be to align technical cyber incident information (from CSIRTs) with military intelligence threat assessments. Create Joint Committee for Cyber Research and Technology Innovation Innovation by the private sector in new cyber technologies is outpacing that of governments, and capacity gaps between governments are also vast. The EU and NATO should create a Cyber Innovation Committee to help address the technology gap between the public and private sectors and reduce the uneven preparedness among member states. The Committee would consist of EU and NATO civilian and military officials, researchers, experts, and technology entrepreneurs, whose task would be to look at the private sector market and identify the innovative tools that are relevant to member states. The Committee would complement the efforts of countries that have already set us similar taskforces at national level, or assist the majority of EU/NATO member states that do not have such capacity. Two fast-developing technological areas would be worth keeping track of. First is the growing issue of cloud computing (and cloud backups) for NATO and EU cyber resilience. On the one hand remote storage can help maintain digital continuity of operations in case of an infrastructure disruption. On the other hand, clouds also have their insecurities and the level of responsibility that private operators bear for the security of their cloud still needs to be better defined. In any case, cloud computing is increasingly finding its way into our everyday lives, the EU–NATO Cyber Innovation Committee should look at better cyber defense capabilities in this field. Second is the growing role of automated information sharing in identifying relevant information more quickly, but also in automating threat mitigation in real time. Automated sharing of security and threat information could help the EU and NATO to standardize their threat information. The Committee could identify adequate information-sharing platforms that can withstand increasingly complex attacks, based on open industry specifications. Such platforms not only enable rapid communication and peer-based sharing, they also help reduce cost and increase the speed of cyber defense by automating processes that are currently often performed manually. Establish a Joint Working Group to Synchronize EU and NATO Crisis Response Systems To date the existing capacity to synchronize EU and NATO cyber crisis response mechanisms is limited. It involves formal and informal meetings between the North Atlantic Council and the EU Political and Security Committee, exchanges at ministerial meetings, cross briefings to respective Committees and Councils, and informal staff-to-staff interaction, for instance between the European External Action Service and NATO’s International Staff. As is true for all forms of collective response in the EU or NATO and especially between the two, better and smoother cooperation in the case of cyber crises would be needed. The EU cyber crisis response mechanisms and NATO’s Crisis Response System should be synchronized in order to respond to major cyber incidents that affect multiple EU member states and NATO Allies or EU/NATO institutions. The recent EU announcement of a “blueprint” to respond to large-scale cybersecurity incidents invites rethinking EU and NATO coordination on this issue. Hence, the EU and NATO should consider establishing a joint working group to propose how to synchronize their systems. As a first step, the Joint Working Group should develop a common template of crisis management phases through the full spectrum of EU and NATO competencies for cyber aspects. The Joint Working Group could also look at clarifying responsibility at the national and supranational levels, for issues like attribution or countermeasures. Proposals should also be made on how to synchronize joint strategic communication among EU and NATO institutions. Finally, more concrete proposals could be developed for using the EU Permanent Structured Cooperation (PESCO) or NATO structures to create national Cyber Defense Automated sharing of security and threat information could help the EU and NATO to standardize their threat information.” “ G|M|F December 2017 5 Policy Brief Rapid Reaction Teams for supporting countries before, during, and after crises. PESCO could provide the possibility of jointly funding rapid reaction capacities for assisting member states in need. Given the existence of different crisis management tools that the EU and NATO have at their disposal, what is crucial now is to align those instruments and to work toward a common EU–NATO playbook on how to react to cyber incidents and crises. Develop a Peer-Assessment Process to Identify Key Resilience and Capability Gaps Cybersecurity and defense are national responsibilities of the EU and NATO member states, and the coordinating role at the supranational level is still limited. The result is an uneven preparedness among member states. The overall consequence of this gap, since our systems are heavily interdependent, is less cybersecurity for all. NATO has adopted the Cyber Defense Pledge that aims to improve NATO Allies’ national cyber defense capabilities in key areas. In parallel, the EU Directive on the security of network and information systems (NIS Directive) forces member states to adopt legal measures to boost the overall level of their cybersecurity by May 2018. The timing may be right to develop a peer-assessment process within NATO and the EU to address key gaps in the cybersecurity and defense of NATO Allies and the EU Member States. Given sensitivities around information sharing, such a process would probably have to be voluntary to start, perhaps following something of a PESCO model, but should aim to soon be broad and comprehensive. The peer-assessment process would map functions of essential services that are critical for the EU and NATO missions and operations and for member states’ national security, as well as their cross-border and cross-sectoral interdependencies. The assessment would produce check lists of vulnerabilities and suggested fixes in participating EU and NATO member states, including their critical economic sectors. One option, among others, could be to use common funding to assist those member states where serious resiliency gaps have been identified, or at minimum, to facilitate voluntary assistance from more advanced nations to those who have invested less in cybersecurity. The EU’s Permanent Structured Cooperation (PESCO) could enable member states to transfer from a strictly voluntary resilience and defense capability-building model to a model of binding commitments. The EU and NATO could also strive, together with able and willing member states, to share best practices and make concrete proposals on how to improve civil-military cooperation and public-private cooperation at the national level.

### Solvency---2NC

#### Solves resources

Lété and Pernik 17. Bruno Lété is a senior fellow for Security and Defense Policy in the Brussels office of The German Marshall Fund of the United States. Piret Pernik is a research fellow at the International Centre for Defence and Security in Tallinn; “EU–NATO Cybersecurity and Defense Cooperation: From Common Threats to Common Solutions”; December 2017; GMF; <https://www.gmfus.org/sites/default/files/EU-NATO%2520Cybersecurity%2520and%2520Defense%2520Cooperation%2520edit.pdf> //BY

Create a Joint Cybersecurity Trust Fund to Build Up Resilience of Partner Countries EU–NATO cybersecurity and defense cooperation with partner nations is a win-win for all sides. Partner nations with the support of the EU and NATO can enhance their own technical cyber capabilities, information networks, and standards, while in return these partners will be able to more efficiently share with the EU and NATO their firsthand information, expertise, and experience. Indeed, the better the technical capacity that partner nations develop, the more they can contribute to EU or NATO collective cybersecurity and defense. A Joint EU–NATO Cyber Trust Fund should be created to address the buildup of local skills, and enable stakeholders in partner nations to attend EU or NATO cyber courses, seminars, trainings and conferences, or to organize similar types of activities in their home land. The Trust Fund can also stimulate the development of local skills by requiring at least one local partner or support team to be involved in the project, rather than simply helping European or American contractors export their technology to the partner nations. The Joint EU–NATO Cyber Trust Fund should encourage partner nations to propose projects themselves, rather than the EU and NATO pre-defining specifics for trust fund projects and proposals. Bundling the efforts of various EU or 7 NATOP Cooperative Cyber Defense Centre of Excellence, “Tallinn Manuel Process,” https://ccdcoe.org/tallinn-manual.html. NATO assistance providers into a Joint Trust Fund would also avoid duplication and better respond to the real needs of partner countries. Today, decisionmakers both in the EU and NATO are increasingly concerned with creating the most efficient capabilities and funding schemes for their partners. There are already genuine examples where the EU and NATO coordinate their financial assistance, such as the regular EU contributions to NATO trust funds for the disposal of unexploded ordinances and anticorruption. In this light, the development of a Joint EU–NATO Cyber Trust fund may not be such a far-fetched idea

#### Solves deterrence better

Lété and Pernik 17. Bruno Lété is a senior fellow for Security and Defense Policy in the Brussels office of The German Marshall Fund of the United States. Piret Pernik is a research fellow at the International Centre for Defence and Security in Tallinn; “EU–NATO Cybersecurity and Defense Cooperation: From Common Threats to Common Solutions”; December 2017; GMF; <https://www.gmfus.org/sites/default/files/EU-NATO%2520Cybersecurity%2520and%2520Defense%2520Cooperation%2520edit.pdf> //BY

Study the Adequacy of Cybersecurity and Defense Concepts and Strategies EU or NATO planning is inwardly focused, revolving around member states’ existing capabilities and institutions, while their adversaries often plan their capabilities around the specific vulnerabilities of the actors they expect to confront. Russian “active measures” in Europe and North America, for example, are designed to exacerbate political tensions and vulnerabilities, such as ethnic relations, regional separatism, or socio-economic or cultural cleavages. In this manner, Russia views the development of cyber capabilities as supporting a broader set of conventional, hybrid, or nuclear capabilities. In this light, there is a real need for the EU and NATO — or an independent academic institution — to take a more outwardly focused approach to studying the cyber strategies and capabilities of NATO and the EU’s potential adversaries or competitors, such as Russia or China, and that puts in perspective the EU and NATO’s own state of play in cyberspace. Such an outward-looking approach toward cybersecurity and defense could serve as a source of inspiration on how to improve EU and NATO cyber strategy and capabilities. As a modern state-on-state conflict is increasingly likely to begin in cyberspace, the EU and NATO must think more actively which cyber capabilities they must develop to more effectively deter — or even retaliate against — their potential adversaries. Develop EU–NATO Triggers for a Joint Response to Cyber-Attacks Leaders in EU and NATO member states are getting more comfortable talking openly about active and reactive joint responses to adversaries in cyberspace. NATO has already recognized a serious cyber-attack as a potential Article 5 trigger, and at its November 2017 defense ministerial, the Alliance announced the creation of a Cyber Operations Center that will facilitate the integration of cyber capabilities with conventional military capabilities. But the current doctrine and crisis management conditions enshrined in NATO and EU cyber policies still puts the emphasis on a defensive posture only. A clearer definition is needed of the circumstances, degree, and manner in which active or counter-measures can or should be taken if EU–NATO member states perceive a cyber threat or suffer a cyber-attack. The authorization to use the EU civilian toolbox or NATO offensive capabilities may be clear if a member state faces a large-scale, devastating cyber crisis. The grey zones are a problem. The Kremlin for instance has clearly been focusing its efforts in the gray zone, and it has gained some sophistication in avoiding lines that would trigger a common response from EU or NATO member states. Russia is also not the only potential adversary capable of similar tactics.6 There is thus an acute need to define when and how the EU and NATO must respond against the day-to-day cyber intrusions that fall below the threshold of being perceived as a clear act of aggression. 6 For example, small to medium scale cyber-attacks on critical infrastructure, hacking of sensitive information, spreading of disinformation. The Kremlin has been focusing its efforts in the gray zone, and it has gained some sophistication in avoiding lines that would trigger a common response from EU or NATO member states.” “ G|M|F December 2017 7 Policy Brief The development of a set of EU–NATO basic principles that would trigger a joint response would be a good first step. The Tallinn Manual published by the NATO CCDCoE could offer inspiration on how the EU and NATO can define these principles while respecting the application of the international law.7 Currently the EU and NATO need to assess each individual cyber threat or cyber-attack on a case-by-case basis without the support of standard measurement tools and indicators that can help them formulate a swift and proportionate response. This considerably slows down the decision-making process. Having a set of pre-agreed basic principles would contribute significantly to efforts at improving reactiveness and resilience at the EU and NATO levels.

#### Solves deterrence/resilience

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

Finally, for EU-NATO cooperation in the field of bolstering resilience more steps are needed, despite the progress that has been achieved since 2016. This is underlined by a recent EP resolution on EU-NATO cooperation, which highlights that, for example, “efforts to create more synergies between civilian and military components, to advance common resilience and hence avert future hybrid threats”﻿[[95]](https://www.clingendael.org/pub/2021/countering-hybrid-threats/4-potential-for-future-eu-nato-cooperation-and-beyond/) are necessary. Some even argue that, at present, the resilience strategies of NATO and the EU are not sufficient in countering hybrid threats.﻿[[96]](https://www.clingendael.org/pub/2021/countering-hybrid-threats/4-potential-for-future-eu-nato-cooperation-and-beyond/) Fortunately, resilience is an area that has a great deal of potential for further cooperation between the EU and NATO, mainly because this area is not yet very politicised.﻿[[97]](https://www.clingendael.org/pub/2021/countering-hybrid-threats/4-potential-for-future-eu-nato-cooperation-and-beyond/)

In general, more effective counter-hybrid efforts would require tailor-made responses, an increased number of (joint) scenario-building exercises and a change of mindset from a reactive to a proactive approach.﻿[[98]](https://www.clingendael.org/pub/2021/countering-hybrid-threats/4-potential-for-future-eu-nato-cooperation-and-beyond/) In addition, suggestions that have been outlined above to enhance cooperation in the areas of crisis response and cyber security and defence will also contribute to enhancing cooperation in the field of bolstering resilience. In particular, this refers to the following suggestions: more regular organisation of joint counter-hybrid exercises (with a specific focus on resilience); a joint EU-NATO taskforce for resilience building; and clarifying the delineation of responsibilities between the EU and NATO.

Another opportunity to enhance cooperation for the benefit of bolstering resilience lies in disaster relief. During the corona pandemic, the ERCC and the EADRCC have demonstrated that advanced cooperation is indeed possible. The EU and NATO should build upon this experience. This should start with exchanging best practices and lessons learned. This could then be a solid foundation for and ease future cooperation. In addition, the number of (joint) crisis management exercises could be expanded. Such exercises should include those scenarios that test the resilience of member states, including hybrid threats, cyberattacks and pandemics. In case a real crisis would occur, the EU and NATO would already have an idea of what is expected and which actions will be required.

In addition, bolstering resilience at the benefit of countering hybrid threats entails more than merely responding to immediate and sudden calamities and crises. One should also take into consideration, amongst other things, general societal resilience, the resilience of critical infrastructure, protecting the stability of democratic systems, and financial and economic resilience. To assess the potential role of the EU and NATO in these domains, their respective toolboxes should be analysed. In this regard, it makes sense that NATO will be responsible for enhancing the resilience of the critical (military) infrastructure of its member states. In contrast, the EU might be better equipped to promote resilience in the societal, financial-economic and political domain. Both organisations should discuss the delineation of responsibilities in the area of resilience.

#### Would use the Estonia model

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

Additionally, synchronisation between the EU and NATO response activities to cyber threats deserves more attention. The EU and NATO could discuss more concretely the delineation of responsibilities and especially of military tasks with regard to cyber threats: when and how should the EU and/or NATO respond to actual cyber threats? For example, a logical division of labour could be an EU focus on enhancing coordination and cooperation among its member states regarding the protection of critical civilian digital infrastructure, while NATO concentrates on enhancing coordination and cooperation among its member states concerning the protection of military digital infrastructure. The focus for both organisations in this regard should be both preventive (sharing threat analysis and protection advice) as well as responsive (in case of actual cyberattacks). The development of a set of EU-NATO basic principles or (non-binding) guidelines on what would trigger a joint response would be a useful step as well. The Tallinn Manual published by the NATO Cyber CoE could offer assistance on how to define these principles while respecting the application of international law.﻿[[93]](https://www.clingendael.org/pub/2021/countering-hybrid-threats/4-potential-for-future-eu-nato-cooperation-and-beyond/) Some experts advocate a common EU-NATO cyber strategy to better align EU-NATO efforts in tackling cyber threats, but currently there seems to be little support for this idea among the member states.﻿[[94]](https://www.clingendael.org/pub/2021/countering-hybrid-threats/4-potential-for-future-eu-nato-cooperation-and-beyond/)

### Say Yes

#### NATO says yes

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

Bruno Lété, of the German Marshall Fund of the United States, also observes improved cooperation between EU and NATO in the field of cyber security. He states that “Since neither organisation possesses the full range of capabilities to tackle contemporary security challenges, there is a serious incentive for the EU and NATO to cooperate in times of crisis. And in the field of cybersecurity and defence the past few years have indeed brought significant change. The EU and NATO share many of the same priorities in cyberspace, their policies are largely identical – based on the principles of resilience, deterrence and defence – and their tools are becoming increasingly complementary.”﻿[[74]](https://www.clingendael.org/pub/2021/countering-hybrid-threats/3-eu-nato-cooperation-what-has-been-achieved-so-far/) Concerning the successes of increased cooperation, Lété mentions exchanges between staff on concepts and doctrines, information on training and education courses, ad-hoc exchanges on threat assessments, cross-briefings, including on the cyber aspects of crisis management, and an annual high-level EU-NATO staff-to-staff dialogue. He also highlights the fact that since 2017 the EU and NATO flagship crisis management exercises – respectively called EU PACE and NATO CMX – are being coordinated and held in parallel with options for the mutual participation of EU and NATO staff.

#### CP solves info sharing controversy

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

However, an additional way to improve information exchange may be the following. In July 2021, the European Parliament (EP) proposed the creation of a common EU-NATO cyber threat information hub, as well as a joint EU-NATO Task Force for cybersecurity, in order to define and agree on collective responses to cyber threats. The EP also called for stronger coordination between the EU Agency for Cybersecurity (ENISA) and the NATO Cooperative Cyber Defence Centre of Excellence and for increased EU-NATO coordination as regards establishing collective attribution for malicious cyber incidents.﻿[[90]](https://www.clingendael.org/pub/2021/countering-hybrid-threats/4-potential-for-future-eu-nato-cooperation-and-beyond/) A recent Clingendael report also advocates transforming the existing NATO Cyber Centre of Excellence in Tallinn into a joint NATO-EU Cyber Centre of Excellence that could provide the main forum for strategic discussions, joint training and exercises.﻿[[91]](https://www.clingendael.org/pub/2021/countering-hybrid-threats/4-potential-for-future-eu-nato-cooperation-and-beyond/) Establishing a completely new institution to further improve EU-NATO cooperation regarding cyber threats does not seem very beneficial﻿[[92]](https://www.clingendael.org/pub/2021/countering-hybrid-threats/4-potential-for-future-eu-nato-cooperation-and-beyond/), yet exploring whether to make existing organisations more ‘joint’ might be worthwhile to further improve information sharing, staff-to-staff contacts, joint workshops and exercises.

# States

### SPP CP

#### SPP solves

Greenhill 22. Jim Greenhill is a Senior PA NCO to the Chief of the National Guard Bureau; “Three Nations, One Goal: Continued Freedom”; June 27, 2022; Air National Guard; <https://www.ang.af.mil/Media/Article-Display/Article/3074655/three-nations-one-goal-continued-freedom/> //BY

VILNIUS, Lithuania – Three Baltic nations are laser-focused on one goal: defending their independence and territorial integrity. The chief of the National Guard Bureau heard the same message in visits to each country, part of a five-nation trip to recognize and strengthen National Guard security cooperation relationships with Eastern European and Baltic nations threatened in the wake of Russia’s brutal, unprovoked invasion of Ukraine. “I am here to reinforce how important these partnerships are,” Army Gen. Daniel Hokanson said. “Security cooperation is one of the most important tasks the National Guard undertakes – and these mutually beneficial partnerships promote both the readiness and teamwork of our respective military forces.” Almost 30 years ago, a seed was planted in the Baltics, a seed that grew beyond the imaginings of the visionary leaders who nurtured it to become the 93-nation Department of Defense National Guard State Partnership Program. In 1993, Estonia, Latvia and Lithuania each partnered with a state National Guard, the first three nations to join the nascent SPP. Three decades on, what started as individual relationships with Maryland, Michigan and Pennsylvania is maturing into a regional grouping: all three countries have access to the training and capabilities of all three states and – through them – to the expertise and resources of the 450,000-strong National Guard across all 50 states, three territories and the District of Columbia. “As the Baltic nations’ military capabilities have matured, so has each partnership,” Hokanson said. The SPP contributed to each nation’s preparations to join NATO. Estonian, Latvian and Lithuanian troops co-deployed multiple times to Iraq and/or Afghanistan with their National Guard partners. The SPP continues to assist as each nation’s armed forces continuously improve their professionalism and modernize their military equipment. Each nation is, of course, also unique: - Estonia is particularly strong in cyber defense, motivated by a 2007 Russian cyberattack that crippled the entire country. It hosts a NATO Cyber Defense Center of Excellence and is the leading member of the alliance for cybersecurity issues. The Maryland National Guard’s Cyber Operations Group has contributed to and learned from the Estonians. – Conscription is still part of Estonia’s and Lithuania’s military design; Latvia has an all-volunteer force. - Estonia also hosts the Baltic Defence College, a joint, senior leader military education institution. - Latvia hosts the NATO Center of Excellence for Strategic Communications, a vital resource given Russia’s relentless misinformation campaign. - Latvia has a proficient Joint Tactical Air Controller capability and was the first NATO country outside the United States to develop JTACs. - In 1990, Lithuania became the first Soviet Republic to declare independence, beginning the collapse of the former Soviet Union. - In 2020, during the COVID-19 pandemic, Lithuania donated personal protective equipment to Pennsylvania as a token of appreciation for their enduring partnership. Each nation borders Russia and shares a painful history of Soviet occupation. Today, Russians brutalize and kill Ukrainians, conduct mass deportations and destroy towns with artillery – the same tactics they used in the Baltics in the 1940s. The three nations have generously contributed to Ukraine’s defense of its homeland and blocked Russian media broadcasting in their countries. Ukrainian flags, posters, murals and other displays of support are common in all three countries, and some troops wear Ukrainian flags under their own flag on their uniforms. During his visits to the three countries, Hokanson met with U.S. ambassadors and the host nations’ senior defense and military leaders. He joined a roundtable discussion in Estonia at the Baltic Defence College and toured cyber defense operations. In Latvia, he visited troops at the Adazi training center, including a multination NATO division headquarters. “Ukrainians are defending our values,” Hokanson was told during his visits. And he was told, “A Russian tank killed in Ukraine won’t come here: This is our war.” And, “There is no way we are going back [to Russian domination.] We would rather die than go back.” Hokanson reassured his counterparts about America’s ironclad commitment to its NATO allies and the National Guard’s commitment to its security cooperation partners. As if to underline the point, while he was there, Vermont National Guard F-35 Lightning multirole fighter jets streaked low along the Baltic coast on a NATO mission defending the skies of Europe. If those who do not know history are condemned to repeat it, that may explain the existence of the Genocide and Resistance Research Centre of Lithuania in Vilnius, which Hokanson visited on the last day of his trip. The center is in a building used first by the KGB, then the Gestapo during the Nazi occupation, and then by the KGB again during the Soviet era. Visitors can tour the cells where Lithuanians were held, tortured and executed. Lithuanians died as recently as 1991: 23 killed and 900 wounded defending the country’s newfound independence. Across the Baltics, the stories handed down by past generations are too horrific, and the memories of many still living too vivid to permit complacency.

# Adv CPs

### Conventional SC Adv CP

#### \*\*\*\*The United States Federal Government should increase its security cooperation with NATO, specifically in the Baltic Area with conventional weapons and forces.

Redo the cp text

#### Conventional security assistance is key, not cyber

Karnitschnig 6-20 (Matthew Karnitschnig, Chief Correspondent at POLITICO Europe. BA in History @ Hampden Sydney College, MS in Journalism @ Columbia. “THE MOST DANGEROUS PLACE ON EARTH”, https://www.politico.eu/article/suwalki-gap-russia-war-nato-lithuania-poland-border/)LR

Despite the Baltics’ strategic concerns, what may be the most dangerous thing about the Suwałki Gap is its relative irrelevance. A move by Russia on Poland or Lithuania would clearly trigger NATO’s Article 5 mutual defense provision, immediately pulling in all the alliance’s members — from Turkey to Bulgaria to France and the United States. At least in theory. How eager would Washington and NATO be to risk Armageddon over a stretch of largely unpopulated farmland few of their citizens even know exists? It’s exactly the kind of edge case that Putin has proved eager to test. Until (and if) Finland joins, Lithuania’s 900-kilometer border with Russia and Belarus is the longest in the alliance. But with an army of just 20,000 and an air force with only five planes including transport aircraft and one single-engine Cessna, Lithuania, like its Baltic neighbors, is ill-equipped for a Russian assault — even with help from the German-led battle group currently stationed in the country. “The only answer to that challenge is an increased NATO presence here,” said Margiris Abukevičius, Lithuania’s vice minister of defense. “We know how Russia is obsessed with closing land corridors.” During a visit to Vilnius earlier this month, German Chancellor Olaf Scholz tried to reassure his hosts of Berlin’s commitment to Baltic security but ended up sowing confusion. Scholz told reporters that Berlin would move “in the direction” of stationing “a robust combat brigade” in Lithuania, implying several thousand troops would be deployed. His aides later walked back the comments, saying that Germany would only move the unit’s headquarters — around 50 personnel — there, while the majority of the troops would remain in Germany. While the U.S.-led alliance has yet to take a final decision, officials have signaled that NATO would significantly bolster forces in the Baltics and elsewhere along the EU’s eastern frontier, heralding a historic shift in NATO posture and shifting the pact’s center of gravity to the east. Though NATO has four 1,000-strong battle groups stationed across the region, Baltic political leaders and military planners argue that much more would be needed to deter Russian aggression. “You have a so-called trip-wire force, but you may as well call it a suicide mission,” said Ilves, who served as Estonian president from 2006 to 2016. The U.S. and Germany long cautioned against such a move, in part because of a 1997 accord, known as the NATO-Russia Founding Act, in which the alliance agreed with Moscow not to establish permanent bases in new member states in “the current and foreseeable security environment.” Russia’s attack on Ukraine, however, has convinced even longtime skeptics of what NATO calls “forward defense” in Eastern Europe that the time has come. “I’ve changed my mind,” said Ben Hodges, a retired American lieutenant general who commanded the U.S. Army in Europe from 2014 to 2017. “Our good faith efforts to engage with Russia have failed.” In Belarus, over which Putin has recently asserted more influence, the Russian military has recently used air bases and other military infrastructure to launch assaults on Ukraine. Hodges said he doubts whether Russia, which is struggling in Ukraine, could muster the capabilities it needs to attack the Baltics for now. But he said it was essential for NATO to use this opportunity to prepare for the worst, including by bolstering the Baltics’ air defenses and ensuring better integration between local forces and the rest of the alliance. He said he could envision a system with a “rotating permanent presence” of NATO forces in the region, similar to how the U.S. operates in South Korea. Another key factor in the region’s defense is Poland, which has the largest military in the region. Historic disputes between Poles and Lithuanians in the Suwałki corridor over language and minority rights on both sides of the border have led to speculation that Putin could use those tensions to his advantage, similarly to his tactic in Donbas, where he succeeded in harnessing pro-Russian sentiment to unleash a separatist movement. That has yet to happen. Cross-border cooperation between the Polish and Lithuanian militaries has never been closer, according to General Rajmund Andrzejczak, Poland’s top military commander. “We see what the Russians are doing in Ukraine, so we don’t trust them,” said the general, who once served in the Suwałki region, stressing that Poland was prepared to honor its alliance obligations towards Lithuania if Russia moves in. “We have to be very, very ready,” he said.

### Cyber CP

#### The United States federal government should coordinate a T-12 technology organization with France, Germany, Japan, United Kingdom, Australia, Canada, South Korea, Finland, Sweden, India and Israel.

#### T-12 solves.

Cohen and Fontaine 20 [Jared Cohen, former member of the U.S. State Department’s Policy Planning Staff. He currently serves as CEO of Jigsaw and is an Adjunct Senior Fellow at the Council on Foreign Relations; Richard Fontaine, CEO of the Center for a New American Security. He has worked at the U.S. Department of State, on the National Security Council, and as a foreign policy adviser to U.S. Senator John McCain; 11-2020; "Uniting the Techno-Democracies"; Foreign Affairs; https://www.foreignaffairs.com/articles/united-states/2020-10-13/uniting-techno-democracies; KL]

FROM MANY, ONE Although the democracies currently suffer from a deficit of cooperation, their capacity to work together endures. Here, history offers useful guidance. In 1973, U.S. Treasury Secretary George Shultz convened the finance ministers of France, the United Kingdom, and West Germany in the White House library for informal talks. This “Library Group” quickly added Japan to become the G-5 and later included first Italy and then Canada to become the G-7. In the decades that followed, this informal group of advanced liberal democracies, which for 16 years included Russia as the G-8, would emerge as a powerful international force. Among other issues, the group coordinated its members’ responses to 9/11 and to the 2008 global financial crisis. Just as the G-7 came to guide multilateral action among the world’s leading economies, a set of techno-democracies—countries with top technology sectors, advanced economies, and a commitment to liberal democracy—must take action on contemporary digital issues. So far, these leading states have acted independently, but their combined market power and national strength would make them a potent unified force. For now, 12 countries stand out for inclusion in such a group. The United States is arguably still the world’s leading technological power, and France, Germany, Japan, and the United Kingdom all have large economies and impressive technology sectors. Australia, Canada, and South Korea have smaller economies, but they are also important players in technology. The same is true of Finland and Sweden, which are telecommunications and engineering powerhouses. India and Israel are also logical candidates for membership, owing to the global reach of their flourishing technology and startup sectors. Given the deep need for coordination among like-minded states, this “T-12” group of techno-democracies would fill a yawning gap in modern technological and geopolitical competition. The T-12’s members would undoubtedly disagree on many issues, but the group could provide a critical venue for them to air their grievances. The United States, in particular, should welcome the participation of others, since their presence at the negotiating table would not only improve its digital advantage but also reduce the sense among these countries that they are merely pawns, rather than partners, in a U.S.-Chinese superpower competition. The most logical structure for the T-12 is an informal group of states, not a secretariat-laden international organization or an alliance with a mutual defense agreement. Although critics often dismiss gatherings such as the G-20 and the Asia-Pacific Economic Cooperation as once-a-year opportunities for heads of state to gather for a few hours, don an ethnically unique shirt, jawbone, and take a group photo, this is a misleading stereotype. Such groupings have in fact been highly effective at marshaling multilateral action. In the wake of 9/11, for instance, G-8 summits produced specific commitments to prevent a repeat attack. It is thanks to the actions taken then that modern commercial aircraft have hardened cockpit doors, major international ports screen cargo containers for dangerous materials, and nations restrict the export of portable surface-to-air missiles. The G-8 was also at the forefront of public health efforts. In 2001, the group established the Global Fund to Fight AIDS, Tuberculosis and Malaria, which has saved millions of lives through investments in research and global health programs. And after the 2008 financial crisis, the G-20 committed to a $5 trillion stimulus package and proposed new financial regulations, helping contain the subsequent recession’s damage and prevent another crash. The government leaders or ministers who meet as the T-12 would also have a unique opportunity to enlist the private sector and international organizations in their work. Annual meetings could serve as an arena for business leaders to join government officials in coordinating responses to emerging issues such as the need to improve remote-learning technology in response to the COVID-19 pandemic and what the future of counterterrorism might look like. The format for these meetings could include issue-based sessions, in which governments invite leading private-sector figures for focused discussions, or standing forums akin to the Asia-Pacific Economic Cooperation’s Business Advisory Council, which provides advice to Pacific Rim leaders on concerns facing businesses throughout the region. The T-12 could also develop working groups and committees on the multistakeholder model, which brings together representatives from business, civil society, government, and research institutions. These groups would then pass recommendations up to ministers and principals. Simultaneously, leaders could collaborate with other multilateral organizations—working with NATO on AI security, for instance, or with the Organization for Economic Cooperation and Development on the industrial implications of disruptive technologies. AN INITIAL AGENDA The success of the T-12 will inevitably hinge on its ability to translate its conceptual appeal into the nuts and bolts of executing a real agenda. One task its members could start with is information sharing. Within the T-12, governments could update one another on the security of supply chains, particularly in critical sectors such as semiconductors, where China aims to dramatically reduce the portion of the market currently controlled by American, Dutch, and Japanese firms. They could conduct audits of supply chains that cross international boundaries, especially those that include Chinese-made components or software. Members could compare their assessments of the risks of China’s 5G technology, examine advances in quantum computing, investigate AI safety, and share strategies for preventing the theft of intellectual property. In a more ambitious step, they could exchange information about online propaganda, disinformation, the integrity of academic research, and specific ways in which autocratic regimes employ technology to erode liberal democracy. Setting standards for the use of emerging technologies would be another crucial job for the T-12. The countries and companies producing the most advanced technology have a valuable first-mover advantage: they can set guidelines for how they expect their products to be used. Facial recognition software would be a good test case for the T-12’s potential on this front. This technology is already being used for surveillance purposes, including by the Chinese government to monitor Uighur Muslims in Xinjiang and by Moscow to link photographs with social media accounts. The leading democracies have yet to agree on rules for using facial recognition technology, including its proper role in the criminal justice system, or the protocols that should govern data collection. The T-12 could address this by exploring how such technology could be used to secure large events or assist in law enforcement investigations, but not as a means of social control or mass intimidation. Autocracies have realized that technology is a central element of modern geopolitical competition. Beyond helping the democracies get on the same page as they compete with China, the T-12 could also serve as a way for members to air differences within the group itself. Europeans might object, for instance, to the fact that Israel’s NSO Group, a controversial technology firm known for its spyware products, sells smartphone surveillance tools to autocracies, and the Americans may disagree with the EU’s focus on privacy when it infringes on free expression. The democracies have varied approaches to data protection, privacy, and free speech. The T-12 would allow them to explore these differences, with the ultimate aim of establishing broad principles, understanding disagreements, and narrowing the gaps between participants. Coordinating investments would represent another natural function of the T-12. Members could rationalize their allocation of resources to innovation and R & D and to securing supply chains. They could even make concrete financial commitments to counter China’s Digital Silk Road and 5G capabilities and launch joint projects in such areas as quantum computing, cybersecurity, and tools for detecting AI-generated counterfeit images or videos known as “deepfakes.” In the realm of more speculative technologies, it could examine advances in 3-D printing, potentially unbreakable encryption methods based on quantum mechanics, and microscopic sensing technology. More ambitious still, it might launch a joint fund to extend loans and loan guarantees to developing nations that seek trusted 5G equipment and other technology that accords with liberal values. Finally, the T-12 could serve as a forum for coordinating policy. Members might harmonize their export controls on cyber-surveillance tools; regulate the use of blockchain, a digital ledger of global transactions, to ensure the integrity of supply chains when it comes to sectors such as defense manufacturing and medical equipment; generate common standards for a variety of 3-D printing methods; and even coordinate their education and immigration policies to develop and retain top technology talent. More broadly, the T-12 should articulate a vision of the future based on innovation, freedom, democratic collaboration, and liberal values. BIGGER AND BOLDER Over time, the T-12 could expand and transform, just as the G-5 became the G-7 and then, temporarily, the G-8. Starting with the initial 12, the T-12 should aim for around 20 members within five years. Additional individual European states, such as Italy and the Netherlands, could be asked to join, without the complexity of including the European Union itself as a member. In Latin America, Brazil and Chile would make obvious candidates, and in Africa, members could include Kenya, Nigeria, and South Africa. Taiwan would also be a useful participant, even if creative diplomacy might be required to deal with the island’s nonstate status. The T-12’s agenda should similarly grow in ambition. Moving beyond its initial objectives, the group could branch out into securing the supply chains for semiconductors. Doing so would involve multilateral export controls on semiconductor manufacturing equipment and technology, an area in which the techno-democracies have a significant lead over China and others. As part of this effort, they could create an international chip fabrication consortium to move semiconductor production out of China and into a T-12 country and provide shared financing for the billions of dollars such a move would require. And as the world faces diminishing returns in the growth of computing power due to the physical limits of existing materials, the group could launch joint R & D projects devoted to a new generation of microelectronics that might jump-start an increase in computing power again. Technology is too important to be left to the technologists. As its portfolio grows, the T-12 should also take a multinational approach to 5G networks. The current telecommunications equipment sector is a Huawei-dominated oligopoly. This presents a major supply chain and security risk, yet China’s state subsidies make it difficult for others to enter the market. The T-12 could support non-Huawei companies, such as Ericsson, Nokia, and Samsung, as they transition to using an open radio access network, or O-RAN, which relies on open interfaces rather than proprietary equipment. This would allow multiple vendors to supply the market with interchangeable telecommunications components. In the future, it could collaborate on 6G alternatives to Chinese hardware well before they are necessary, helping avoid the very dilemma many economies are now facing with 5G. The T-12 could also develop the framework for a digital currency that preserves the central role of the U.S. dollar in the global financial system. That role is under threat. China’s central bank is already piloting a digital currency program. If the effort succeeds, China is likely to extend its use to countries that participate in its Belt and Road Initiative, expanding the renminbi’s reach as an international medium of exchange and possibly threatening the dollar’s preeminent status. Pursuing a secure digital dollar-based platform would level this playing field, making it faster and easier to accomplish tasks such as moving money between banks, trading oil futures, and tracking money laundering. Beyond this, the T-12’s members could develop and adopt a cyber-deterrence doctrine. The world faces a perpetual threat from cyberattacks, given the low barriers to entry and the difficulty of attributing an attack to a defined actor. To tackle the threat, the T-12 could lay out uniform standards for appropriate behavior in cyberspace and define what constitutes a proportionate response to a cyberattack. Members could cooperate in detecting and measuring attacks by increasing information sharing and establishing early warning mechanisms, then work together to attribute violations to a particular aggressor. And once a culprit is identified, the T-12 could coordinate a joint response. ADDRESSING THE SKEPTICS Objections to a T-12 are easy to imagine. The most obvious would be general opposition to any new international grouping, which would join a raft of existing multilateral organizations, some of which are obsolete. Yet the T-12’s novelty is what makes it relevant. There is no group of advanced democracies to coordinate technology policy: the G-7 leaves out important technology leaders, and the G-20 includes the illiberal states of China, Russia, Saudi Arabia, and Turkey. NATO is a military alliance focused first and foremost on European security. The Organization for Economic Cooperation and Development, with 37 member states, is too large and lacks the track record to break ground on technological issues. The T-12, by contrast, would bring together the right members while elevating technology to a level commensurate with such issues as European security and global economic policy. The private sector’s role in a potential T-12 raises another question: Why would any business participate in a government-driven process? The answer is that it would make economic sense. Consider the inevitable restructuring and geographic diversification of supply chains that will almost certainly follow the coronavirus pandemic. Already, governments and firms are considering reshoring pharmaceutical and medical device production, and firms that are facing factory shutdowns due to the pandemic are rediscovering the merits of diverse supply chains. Multilateral coordination among national governments would make this process less disruptive, costly, and lengthy than it would otherwise be.

#### AT: Russia

Cohen and Fontaine 20 [Jared Cohen, former member of the U.S. State Department’s Policy Planning Staff. He currently serves as CEO of Jigsaw and is an Adjunct Senior Fellow at the Council on Foreign Relations; Richard Fontaine, CEO of the Center for a New American Security. He has worked at the U.S. Department of State, on the National Security Council, and as a foreign policy adviser to U.S. Senator John McCain; 11-2020; "Uniting the Techno-Democracies"; Foreign Affairs; https://www.foreignaffairs.com/articles/united-states/2020-10-13/uniting-techno-democracies; KL]

Then there is the likely reaction of China and Russia. Wouldn’t a new group of techno-democracies merely provoke them? Indeed, they probably would treat it as a threat, but the cost of forgoing cooperation among liberal democracies is far higher than the consequences of any pushback. As the COVID-19 pandemic has proved, when liberal democracies fail to work together, whether, in this case, in harmonizing travel restrictions, employing disease-mitigation measures, or assisting poorer nations, China benefits. The T-12 should not ignore illiberal states, and it can try to work with them on issues such as AI safety or technological responses to climate change. But it should tread carefully and limit their involvement. Ultimately, the world will be safer, more stable, and freer if liberal democracies stick together.

#### AT: Say no

Cohen and Fontaine 20 [Jared Cohen, former member of the U.S. State Department’s Policy Planning Staff. He currently serves as CEO of Jigsaw and is an Adjunct Senior Fellow at the Council on Foreign Relations; Richard Fontaine, CEO of the Center for a New American Security. He has worked at the U.S. Department of State, on the National Security Council, and as a foreign policy adviser to U.S. Senator John McCain; 11-2020; "Uniting the Techno-Democracies"; Foreign Affairs; https://www.foreignaffairs.com/articles/united-states/2020-10-13/uniting-techno-democracies; KL]

A final objection would be based on realism. Cooperation in other fields—global health, say, or economic policy—is hard enough, and the likelihood of building a successful body focused on technological collaboration may be low. Indeed, one should not overstate the degree of like-mindedness among any group of sovereign states, democracies or not. But that is a reason to experiment with new structures to deal with tough problems, rather than rely on either outdated mechanisms or an every-country-for-itself approach. The status quo is not sustainable. If the democracies fail to act, technology will help shift the balance of economic, military, and political power in favor of autocracies.

#### Now is key

Cohen and Fontaine 20 [Jared Cohen, former member of the U.S. State Department’s Policy Planning Staff. He currently serves as CEO of Jigsaw and is an Adjunct Senior Fellow at the Council on Foreign Relations; Richard Fontaine, CEO of the Center for a New American Security. He has worked at the U.S. Department of State, on the National Security Council, and as a foreign policy adviser to U.S. Senator John McCain; 11-2020; "Uniting the Techno-Democracies"; Foreign Affairs; https://www.foreignaffairs.com/articles/united-states/2020-10-13/uniting-techno-democracies; KL]

TIME FOR ACTION

In July 1944, delegates of the Allied countries came together in New Hampshire for what became known as the Bretton Woods conference. After discussions of various technical issues and sweeping foreign policy debates, the conference produced a blueprint for governing the postwar international monetary and financial order. The Allies agreed on a system of fixed but adjustable exchange rates, laid the groundwork for the International Monetary Fund and the World Bank, and embraced an open international economic system. The framework designed then largely remains in place today.

Some of the most pressing technological issues facing the world’s democracies now may ultimately rival in importance the economic issues considered by the Bretton Woods delegates. Just as in 1944, when the United States and like-minded countries recognized that they could no longer make economic policy in a vacuum, today they must recognize that the time has passed when they can deal with the profound effects of technology on their own. For too long, national approaches to technological questions have been ad hoc, poorly coordinated, and left to technology experts to sort out. But in today’s competitive global environment, technology is too important to be left to the technologists.

#### More evidence

Cohen and Fontaine 20 [Jared Cohen, former member of the U.S. State Department’s Policy Planning Staff. He currently serves as CEO of Jigsaw and is an Adjunct Senior Fellow at the Council on Foreign Relations; Richard Fontaine, CEO of the Center for a New American Security. He has worked at the U.S. Department of State, on the National Security Council, and as a foreign policy adviser to U.S. Senator John McCain; 11-2020; "Uniting the Techno-Democracies"; Foreign Affairs; https://www.foreignaffairs.com/articles/united-states/2020-10-13/uniting-techno-democracies; KL]

At the outset of the digital age, democracies seemed ascendant. The United States and like-minded countries were at the cutting edge of technological development. Policymakers were pointing to the inherently liberalizing effect of the Internet, which seemed a threat to dictators everywhere. The United States’ technological advantage made its military more potent, its economy more prosperous, and its democracy, at least in theory, more vibrant. Since then, autocratic states have caught up. China is at the forefront, no longer a mere rising power in technology and now an American peer. In multiple areas—including facial and voice recognition, 5G technology, digital payments, quantum communications, and the commercial drone market—it has surpassed the United States. Leaders in Cuba, Iran, North Korea, Russia, Venezuela, and elsewhere are increasingly using technology for illiberal ends, following China’s example. And despite the United States’ remaining advantage in some technologies, such as artificial intelligence (AI) and semiconductor production, it has fallen behind China in formulating an overall strategy for their use. Almost in parallel, the United States and its allies have stepped away from their tradition of collaboration. Instead of working together on issues of common interest, they have been pulled apart by diverging national interests and have responded incoherently to autocratic states’ co-optation of new technologies. Although officials in most democratic capitals now acknowledge the profound ways in which new technologies are shaping the world, they remain strangely disconnected from one another when it comes to managing them. Coordination, when it occurs, is sporadic, reactive, and ad hoc. The liberal democracies are running out of time to get their act together: whoever shapes the use of emerging technologies such as AI, quantum computing, biotechnology, and next-generation telecommunications will have an economic, military, and political advantage for decades to come. But the world’s advanced democracies have something the autocracies don’t: a long history of multilateral cooperation for the benefit of all. Because the issues are so diverse, what’s needed now is not more piecemeal solutions but an overarching forum in which like-minded countries can come together to hammer out joint responses. This new grouping of leading “techno-democracies”—call it the T-12, given the logical list of members—would help democracies regain the initiative in global technology competition. It would allow them to promote their preferred norms and values around the use of emerging technologies and preserve their competitive advantage in key areas. Above all, it would help coordinate a unified response to a chief threat to the global order. AUTOCRACIES IN THE LEAD Washington has struggled to develop a coherent vision to guide its global technological role, but many autocracies have not. China, in particular, has recognized that the existing rules of the international order were largely written in a predigital age and that it has an opportunity to write fresh ones. Already, Beijing is pursuing this goal by quickly building top-notch capabilities and deploying them throughout the global market, especially in areas where the U.S. presence is weak or virtually nonexistent. In Zimbabwe, for instance, the Chinese AI company CloudWalk is helping develop a national facial recognition system, giving the local government a powerful new tool for political control. But forward-looking efforts such as these are not solely unilateral. China, Russia, and other autocracies are already coordinating around a self-interested global vision. They are shaping standards for the use of new technologies in exclusive groups such as the Shanghai Cooperation Organization, whose members have agreed to collaborate on information security, robotics, and e-commerce, among other areas. They also work through global forums such as the International Telecommunication Union, where some of the same countries have supported international standards that facilitate unaccountable surveillance. Unlike many liberal democracies, quite a few autocracies have realized that technology, including the power to innovate, set norms for its use, and shape the institutions that decide how it will be employed, is not simply a niche functional issue buried in a crowded foreign policy agenda; it is a central element of modern geopolitical competition. The United States, on the other hand, has been mostly reactive. China’s rapid progress in 5G, AI, and quantum communications has stumped multiple U.S. administrations. Washington has no easy answer to China’s so-called Digital Silk Road, an array of technological infrastructure projects to accompany the construction projects of its Belt and Road Initiative, nor does it have an answer to the country’s campaign to establish a digital currency. The United States and its allies have consistently struggled to define the rules of engagement around cyberattacks and have responded inadequately to the use of technologies by autocracies to oppress their people. U.S. officials often complain about Beijing’s dominance in technical standard setting and allies’ deferential attitude toward Chinese infrastructure. But they have had a difficult time changing the nature of the game. The T-12 would help democracies regain the initiative in global technology competition. This is a multinational failure. Liberal democracies around the world simply do not work together on many of the issues that should unite them. Their responses to autocracies’ abuse of technology tend to be fragmented. National interests diverge, disagreements among states arise, and nothing gets done. Within countries, paralysis often occurs as domestic authorities clash with their national security counterparts over how to deal with election meddling, disinformation, and hacking. Instead of pursuing broad collaboration, the liberal democracies have come up with a patchwork of discrete responses: Canada and France’s collaboration on an expert panel tasked with monitoring developments in AI policy, for example, or NATO’s pursuit of a cyber-deterrence doctrine. The dispute over the Chinese telecommunications giant Huawei’s 5G capabilities is perhaps the best example of democracies’ inconsistent response. Following Australia’s initial lead, the United States took a hard line against the company, banning Huawei components from its national 5G network and forbidding U.S. entities from doing business of any sort with it. The United States proceeded to insist that other democracies follow suit, even threatening to withhold critical intelligence from allies if they adopted Huawei products. Still, Washington remains relatively isolated in its opposition. Many governments continue to resist U.S. pressure, pointing out that there is no low-cost, one-stop-shop alternative to Huawei’s technology. Even Canada and South Korea, close U.S. allies, have defied Washington and are considering Huawei equipment for their 5G infrastructure. The democracies have come up with a similarly disjointed response to Russia’s election meddling. Although the Kremlin has interfered in the elections of multiple countries, the problem has largely been treated as a national one, deserving of only a unilateral response from any given target. When Russia interfered in the 2016 U.S. presidential election, only the United States responded with punitive measures. Likewise, Russia’s reported meddling in this year’s U.S. presidential election has so far not produced any unified reaction. Compare that to the response to Russia’s annexation of Crimea and its poisoning of a former intelligence officer and his daughter in the United Kingdom. In those cases, the major democracies coordinated a joint response, imposing new sanctions and expelling Russian diplomats.

# Turkey DA

### Link

#### Turkey hates NATO cooperation with the Baltics

Emmott and Irish 20 (Robin, Reuters diplomatic correspondent in Brussels covering NATO, EU defence and foreign policy, while keeping a special eye on relations with China and the U.S. John Irish, Senior Correspondent at Reuters News with focus on foreign policy. “Turkey still blocking defence plan for Poland, Baltics, NATO envoys say”, https://www.reuters.com/article/us-nato-france-turkey-plans/turkey-still-blocking-defence-plan-for-poland-baltics-nato-envoys-say-idUSKBN23O1TN)LR

BRUSSELS/PARIS (Reuters) - Turkey continues to block a NATO defence plan for Poland and Baltic states despite a deal last year between Turkey’s president and allied leaders, three allied diplomats and a French defence official said on Wednesday. Diplomats said while Ankara has approved the plan, known as Eagle Defender, it has not allowed NATO military chiefs to put it into action. The dispute, first reported by Reuters in November, is a sign that divisions remain between Ankara, Paris and Washington over Turkey’s offensive last year in northern Syria and that frictions over broader NATO strategy have not been resolved. The Turkish government did not immediately respond for request for comment. NATO defence ministers are due to meet later on Wednesday and Thursday via secure video call. “Turkey is refusing to accept these plans unless we recognise the PYD/PKK as a terrorist entity,” a French defence official said, referring to Syrian and Turkish Kurdish groups that Ankara regards as dangerous rebels. “We say no. We need to show solidarity for eastern allies and it’s not acceptable to block these plans,” the official said. At a NATO summit in December, Turkish President Tayyip Erdogan agreed with NATO Secretary-General Jens Stoltenberg and other allied leaders to drop such demands. Turkey began its offensive in northern Syria after the United States pulled 1,000 troops out of the area in October. Ankara’s NATO allies have said the incursion undermines the battle against Islamic State militants. The plan for the Baltic states and Poland, drawn up at their request after Russia annexed Crimea from Ukraine in 2014, has no direct bearing on Turkey’s strategy in Syria, but it raises issues about security on all of NATO’s frontiers. Under the North Atlantic Treaty Organisation’s 1949 founding treaty, an attack on one ally is an attack on all, and the alliance has military strategies for collective defence across its territory.

# Security K

### Security K

#### Baltics threat con literally causes mental health problems.

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]

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.