# Advantage Answers

## Squo solves

### Article 5

#### Squo solves Article 5 – certain lower level attacks invoke Article 5 while the rest are case-by-case

**Machi**, reporter @ defense news, **2021**

(Vivienne, named the Defence Media Awards' best young defense journalist, “NATO looking at holistic path to boost cyber defense arsenal,” Defense News, Dec 14, 2021, <https://www.defensenews.com/global/europe/2021/12/14/nato-looking-at-holistic-path-to-boost-cyber-defense-arsenal/>, accessed 7/3/2022, gdi-tmur)

The new NATO cyber policy released in June also affirms the alliance’s decision to consider that certain “lower-level” malicious cyber attacks by the same threat actor can be as destructive as a single, large-scale cyber attack, and could, at least in theory, trigger the treaty’s Article V collective defense mechanism.

“We see that a lot of activity, ongoing activity below that threshold of one single large attack, can actually have the same strategic conflict implications or more,” van Weel explained. “It’s about not limiting our options to just waiting for a massive attack. It’s about recognizing that what happens below that threshold of a massive attack is worthy of our attention.”

Whether Article V is triggered or not has been and remains a decision made on a case-by-case basis, and should be seen as an added deterrent for potential threat actors, he noted. “The new policy … that’s not escalating. That is just stating clearly how we see the field.”

### CYOC good – general

#### CYOC effective now and NATO Strategic Concept debate reflects evolving commitments to cyber as essential function

**Maigre, 2022**

[Merle, senior cybersecurity expert at e-Governance Academy in Estonia. In 2017–2018, she served as director of the NATO Cooperative Cyber Defence Center of Excellence (CCDCOE), “NATO IN A NEW ERA: GLOBAL SHIFTS, GLOBAL CHALLENGES NATO’s Role in Global Cyber Security” German Marshal Fund APRIL 06, 2022 <https://www.gmfus.org/news/natos-role-global-cyber-security> accessed jcp-TM 6/8]

The Alliance’s Achievements in Cyber So Far Over the past fifteen years, NATO’s approach to cyber issues has evolved from addressing cyber defense in primarily technical terms to viewing it as essen- tial to the alliance’s strategic context. The need to “strengthen capabilities and to defend against cyber- attacks” was first acknowledged by allied leaders at their 2002 summit meetings in Prague.19 However, after Estonia’s digital infrastructure was hit by cyber- attacks in 2007, NATO admitted that a confrontation between states might involve a cyber dimension, and at the Bucharest Summit in 2008 adopted its first cyber-defense policy. The 2008 conflict between Russia and Georgia demonstrated that cyberattacks have the potential to become a major component of conventional warfare. In parallel, the NATO Cooperative Cyber Defence Centre of Excellence (CCDCOE) was accredited as a NATO Centre of Excellence in 2008. Since then, it has grown into a strong, international knowledge hub for cyber defense, bringing together top cyber experts across fields—government, military, industry, and academia—from 29 nations for interdisciplinary research, training, and exercises in four focus areas: technology, strategy, operations, and law. The center connects a trusted community of like-minded states who wish to share information and expertise in cyber security. CCDCOE’s best-known projects are Locked Shields, one of the world’s largest and most comprehensive cyber-defense exercises; the annual cyber conference CyCon; and the Tallinn Manual, which looks at cyber operations within the context of international law. At the 2012 NATO summit in Chicago, allied leaders reaffirmed their commitment to improving the alliance’s cyber defenses by bringing all of NATO’s networks under centralized protection. At the 2014 Wales summit, NATO recognized that international law applies in cyberspace and declared that, since the impact of a cyberattack could be as harmful to modern societies as a conventional attack, cyber defense is a part of NATO’s collective defense mandate. Thus, NATO acknowledged that cyberspace is an operational domain for potential adversaries. NATO’s 2016 Warsaw summit resulted in a decla- ration recognizing that cyberspace has evolved into a separate domain of military operations, in which the alliance “must defend itself as effectively as it does in the air, on land, and at sea.” The subsequent roadmap included the drafting of a NATO cyber operations doctrine, as well as the development of military cyber capabilities. In January 2020, the Allied Joint Doctrine for Cyberspace Operations was published “to plan, execute, and assess cyberspace operations in the context of allied joint operations.”20 At the Warsaw summit, NATO heads of state and government signed a Cyber Defence Pledge, in which they outlined how nations protect their cyber networks. NATO developed detailed questionnaires and metrics related to the pledge and uses them to regularly report on how each nation delivers on its cyber commitments. Allies also discussed how to strengthen the cyber component of NATO’s Command Structure. The Command Structure is the military backbone of the alliance; it is what makes NATO unique. NATO has continuously adapted its Command Structure over the past decades to take account of a changing secrity environment. In February 2018, NATO defense ministers established the Cyberspace Operations Centre (CyOC) as part of NATO’s SHAPE Command Structure, with the aim of integrating the allies’ cyber capabilities into NATO military-operations planning. CyOC is the first cyber-dedicated entity within the Command Structure. The “eyes and ears” of the respective commanders in cyberspace, CyOC aims at enhancing situational awareness in cyberspace and helping integrate cyber into NATO’s planning and operations at all levels. While CyOC operates within the existing NATO frameworks, its main aim is to equip the Supreme Allied Commander Europe with any necessary tools to operate in cyberspace.21 As CyOC moves toward initial then final operating capacity, it will be critical that it is staffed with suffi- cient—and sufficiently expert—personnel.22 During NATO’s July 2018 summit, the allies affirmed, for the first time, their determination “to employ the full range of capabilities, including cyber, to deter, defend against, and counter the full spec- trum of cyber threats,” shifting away from securing cyberspace with defensive measures only. The “full range” of cyber capabilities means that both defensive and offensive capabilities can be deployed by NATO, in line with its defensive mandate and in accordance with international law. As NATO will not develop or acquire any offensive capabilities, it will rely, like in other operational domains, on the voluntary contribu- tions of allies. In late 2020, a team of experts appointed by NATO Secretary General Jens Stoltenberg and chaired by Thomas de Maiziere of Germany and Wes Mitchell of the United States gave their recommendations on how NATO could enhance its political role and better coor- dinate military tasks and political strategies among its members. In 2021, Stoltenberg’s NATO 2030 included eight of those recommendations to guide the revision of NATO’s Strategic Concept.23 At the Brussels summit in 2021, the allies endorsed a new Comprehensive Cyber Defense Policy high- lighting collaboration as necessary to strong cyber defense, which recognized that “the impact of signif- icant malicious cumulative cyber activities might, in certain circumstances, be considered as amounting to an armed attack.24 A key feature of the new policy is the prominent role of offensive cyber operations.25 In Brussels, member states committed to “employ the full range of capabilities at all times to actively deter, defend against, and counter the full spectrum of cyber threats.”26 In other words, the alliance declared it could respond to malicious cyber activities below the threshold of use of force causing significant harm with, among other things, conventional military or offensive cyberspace operations. NATO has committed to develop its next Strategic Concept for the 2022 summit. The alliance’s current Strategic Concept dates back to the Lisbon summit in 2010. It is clearly out of date, having been conceived when terrorism and energy cut-offs were the major threats and the alliance’s primary mission was to culti- vate partnerships with non-member states rather than to face aggressive great-power rivals.

### SQuo solves – international partnerships

#### Squo solves – US engaged in cyber partnerships under persistent engagement and defend forward

**Smeets,** ETH Zurich, Center for Security Studies, **2020**

[Max “U.S. Cyber Strategy of Persistent Engagement & Defend Forward: Implications for the Alliance and Intelligence Collection” Intelligence and National Security vol 35, 2020 – Issue 3, Taylor and Francis Online accessed 7/5/2022 GDI-TM]

Benefits and the creation of partnerships

The strategy of persistent engagement and defend forward can help less capable cyber actors defend themselves against adversaries. Both the U.S. Cyber Command vision and the DoD cyber strategy stress the importance of working closely with international and private sector partners to successfully operate in cyberspace.xxix The DoD strategy states the following: “Our strategic approach is based on mutually reinforcing lines of effort to build a more lethal force; compete and deter in cyberspace; expand alliances and partnerships; reform the Department; and cultivate talent.”xxx On international partnerships, it more explicitly states: “Many of the United States’ allies and partners possess advanced cyber capabilities that complement our own. The Department will work to strengthen the capacity of these allies and partners and increase DoD’s ability to leverage its partners’ unique skills, resources, capabilities, and perspectives. Information-sharing relationships with allies and partners will increase the effectiveness of combined cyberspace operations and enhance our collective cybersecurity posture.”xxxi

The United States has also signed several memoranda of understanding and over the years addressed cyber cooperation in some way, shape or form. In 2008, a MoU was signed between the Department of Defense and the German Federal Ministry of Defence about computer network defense and information assurance.xxxii A year later, a similar MoU on computer network defense was signed with South-Korea. xxxiii

More recently, the Cyber Command worked alongside Montenegrin cyber defenders with as aim “to increase interoperability, build partner capability, and deter malign influence on the democratic processes of our allies, partners and the U.S.”xxxiv It was reported that U.S. Cyber Command personnel operated in the networks of Ukraine and Macedonia as well to help those countries defend against malicious cyber activity.xxxv At the 2019 Cyber Command symposium, specific examples were discussed on how cooperation can also help in not just detecting or deterring adversaries but also cause friction in their operational activity.xxxvi For example, the U.S. might upload foreign APT malware samples on VirusTotal, an online malware repository and file scanning service, forcing adversaries to go back to the drawing broad and adapt.xxxvii One can think of several other scenarios how international partnerships (also with the private sector) can help to ensure more coordinated take down of adversarial operations - actions beneficial to both the US and its partners.

## Cyber

### Threats overblown – minor impact

#### Cyber threats are overblown – attacks often minor and manageable threats

Mueller, 2022

[John, Political Scientist at Ohio State University and a Senior Fellow at the Cato Institute, “The Cyber-Delusion: Digital Threats Are Manageable, Not Existential”, Foreign Affairs, 3/22/22, https://www.foreignaffairs.com/articles/russia-fsu/2022-03-22/cyber-delusion, accessed 7/4/22, GDI-cc]

When Russian forces launched their invasion of Ukraine last month, governments and experts worldwide warned about the danger of catastrophic cyberattacks. Indeed, in the days leading up to Moscow’s invasion, hackers defaced Ukrainian websites, unleashed malware on government systems, and targeted the country’s banking system—albeit with limited effect. Although no cyber-Armageddon has materialized, officials increasingly fear that Russia might eventually step up its efforts and even target the United States.

Russia’s invasion is no doubt catastrophic. But in reacting to it and preparing for what comes next, leaders in Washington and elsewhere should eschew the alarmism that has long warped cybersecurity policy. Mike Mullen, then chairman of the Joint Chiefs of Staff, claimed in 2011 that “the single biggest existential threat out there, I think, is cyber.” The following year, his successor, Martin Dempsey, noted that “a cyberattack could stop our society in its tracks.” Former Defense Secretary Leon Panetta sternly warned in 2012 of an impending “digital Pearl Harbor.” Nicole Perlroth, a cybersecurity reporter at The New York Times, has routinely asked insiders when “a cyber-enabled cataclysmic boom will take us down” and has always been told “18 to 24 months.” She began her survey well over 100 months ago.

This contemporary approach to cyberthreats resembles the aftermath of 9/11, when almost all experts believed an even larger terrorist attack would soon take place. Then, as now, the threat is overblown. Although occasionally dramatic, cyberattacks have turned out to be a comparatively minor and manageable threat. Far too much discussion around the issue focuses on worst-case scenarios, fails to contextualize the problem, and neglects to weigh the costs of cyberattacks against the enormous value of the Internet and artificial intelligence. Most commentary, moreover, does not fully appreciate the ability of the business sector—by far the most tempting of targets for malevolent hackers—to develop effective countermeasures.

### Threats overblown – fixes

#### Cyber alarmists do not assess longer term impact effectively – fixes to viruses and hacks

Mueller, 2022

[John, Political Scientist at Ohio State University and a Senior Fellow at the Cato Institute, “The Cyber-Delusion: Digital Threats Are Manageable, Not Existential”, Foreign Affairs, 3/22/22, https://www.foreignaffairs.com/articles/russia-fsu/2022-03-22/cyber-delusion, accessed 7/4/22, GDI-cc]

The achievements of cyber-sabotage have also been quite modest. The United States and Israel famously used a computer virus known as Stuxnet to hamper Iran’s progress toward developing a nuclear weapon. Although observers hailed the operation as a dangerous new development in modern conflict, the damage proved temporary. Iran quickly rebuilt its centrifuges, and the attack actually proved counterproductive, as it encouraged Tehran to accelerate its nuclear program. There have also been efforts by the United States to physically interfere with missile development in North Korea. Yet, much like the Iranians, Pyongyang eventually solved whatever the problem was, and the attacks had little long-term effect on their program.

Cyber-alarmists have also warned about hackers disabling major infrastructure such as power grids—potentially crippling entire countries. Grids do go down occasionally, but the culprits are typically squirrels and lightning. Regardless of the source, such disruptions are usually brief and bearable, and engineers are increasingly designing systems that are resilient to such threats. Estonia, for instance, the victim of a major and oft-discussed cyberattack in 2007, is now the home of NATO’s Cooperative Cyber Defence Centre of Excellence.

### Threats overblown – no cyber terrorism

#### Cyberterrorist threats overstated – no terrorist group has ever launched a successful cyberattack and standard warfare more effective

Mueller, 2022

[John, Political Scientist at Ohio State University and a Senior Fellow at the Cato Institute, “The Cyber-Delusion: Digital Threats Are Manageable, Not Existential”, Foreign Affairs, 3/22/22, https://www.foreignaffairs.com/articles/russia-fsu/2022-03-22/cyber-delusion, accessed 7/4/22, GDI-cc]

Fears that terrorist groups could inflict damage through cyberspace have been around for many years. And although cyber played no direct role in the execution of the 9/11 terrorist, the event stirred anxiety about the issue. In 2002, for instance, The Washington Post published a lengthy front-page article conveying the views of “government experts” that “terrorists are at the threshold of using the Internet as a direct instrument of bloodshed.”

To date, however, no terrorist group has launched a successful cyberattack. And even if it becomes possible for hackers to shed blood, shootings and bombings are likely to accomplish the same goal far more reliably. Still, cyber has undoubtedly proved to be a relatively convenient method for terrorist groups to recruit and communicate. Rather than creating a paradigm shift, however, this technique has simply replaced or embellished older methods. Even comparatively savvy groups such as the Islamic State (also known as ISIS) tend to comically fail when using the Internet to stir up violence and instruct potential sympathizers. In one case, an ISIS handler connected his eager American charge to a prospective collaborator who happened to be an FBI operative.

For the most part, any virtual terrorist army in the United States has, as terrorism expert Brian Jenkins puts it, remained exactly that: virtual. “Talking about jihad, boasting of what one will do, and offering diabolical schemes egging each other on is usually as far as it goes,” he noted. Indeed, the foolish willingness of would-be terrorists to describe their aspirations and often-childish fantasies on the Internet has often helped police seeking to track them down.

### Threats overblown – limited cyber crime impact

#### Cybercrimes are exaggerated – attacks are remarkably small compared to other forms of illegal activity and businesses are adapting to these threats

Mueller, 2022

[John, Political Scientist at Ohio State University and a Senior Fellow at the Cato Institute, “The Cyber-Delusion: Digital Threats Are Manageable, Not Existential”, Foreign Affairs, 3/22/22, https://www.foreignaffairs.com/articles/russia-fsu/2022-03-22/cyber-delusion, accessed 7/4/22, GDI-cc]

Despite the overheated rhetoric about war, terrorism, election interference, and critical infrastructure, most cyberattacks target the private sector, seeking to steal or extort money from businesses and their customers. The record here, however, is rather encouraging, and it likely has broader relevance. To be sure, cybercriminals have stolen and extorted billions of dollars from businesses and individuals, but firms have done well at limiting the damage by closing software holes, maintaining backups, and safeguarding sensitive material.

A central issue for potential hackers is the profitability of their enterprise. A report by the cybersecurity firm Symantec estimates that 978 million people were affected by cybercrime in 2017, losing $172 billion in total. That number—regardless of how hackers divvy up the profits—is actually remarkably small compared to losses from other forms of illegal activity. Personal and property crimes in 2017, for instance, cost Americans $2.6 trillion.

Businesses are also learning to adapt. Andrew Odlyzko, former head of the University of Minnesota’s Digital Technology Center, points out that many firms have realized they can readily mitigate the most damaging effects of cybercrime through minor and incremental alterations to their business practices. Banks, for instance, increasingly require customers to verify large or suspicious transactions through voice calls or texts. And even though criminals routinely capture millions of credit card numbers through compromised databases, the overall damage is limited and often dominated by the cost of providing replacement cards. Businesses have also made it easy for consumers to recover from fraud.

## Deterrence

### Deterrence fails – complexity

#### Deterrence failure in Ukraine demonstrates the complexity of deterrence – multiple actions required to shore up deterrence

**SMITH** former NATO deputy supreme allied commander for Europe**, and BET-EL,** senior associate fellow at the European Leadership Network, **2022**

[RUPERT and ILANA, “Restoring Deterrence” Project –Syndicate, May 19, 2022 [https://www.project-syndicate.org/commentary/restoring-nato-western-deterrence-against-aggressors-by-rupert-smith-and-ilana-bet-el-2022-05 accessed 7/5/2022](https://www.project-syndicate.org/commentary/restoring-nato-western-deterrence-against-aggressors-by-rupert-smith-and-ilana-bet-el-2022-05%20accessed%207/5/2022) GDI-TM]

The fact that Russia followed through with its threatened invasion of Ukraine demonstrates that NATO and the wider West’s deterrence strategy was no longer fit for purpose. Looking ahead, deterrence must be approached more comprehensively, with policymakers recognizing that it extends far beyond the battlefield.

BRUSSELS – As NATO military chiefs meet in Brussels to discuss the war in Ukraine, the other issue on their minds is the alliance’s forthcoming Strategic Concept, which will shape its priorities for years to come. And here, Russia’s behavior has demonstrated that re-establishing deterrence must play a central role.

When Russia began amassing troops on Ukraine’s border late last year, it embarked on a path of aggression against not just Ukraine but also what it calls the “collective West,” particularly the European Union and NATO. Russia was seeking to deter Ukraine and the West from increased collaboration, while the West was seeking to deter Russia from aggression. The subsequent invasion stems from a massive failure of deterrence.

The Ukrainians have marshalled an impressive defense, and the EU, NATO, and other Western partners and allies have continued to tighten economic and financial sanctions and provide aid. But we are in a dangerous cycle of escalation. The situation demands credible deterrence that goes far beyond the traditional “nuclear umbrella.”

After all, deterrence is not only about nuclear warfare. It is relevant to all forms of confrontation – whether in business or on the battlefield. Many of these dynamics are present in the current conflict. Russia and Europe’s codependent energy relationship had been deemed a strong deterrent on both sides; but it patently failed.

Deterrence is about convincing an opponent that not doing something is in its best interests. Russia first attempted to deter Ukraine and the West by deploying its troops along Ukraine’s borders. But as it did, the United States and its NATO allies released daily intelligence and data revealing Russian troop movements, demonstrating clearly to the Kremlin that they knew what it was doing. Such signaling is the first element of deterrence.

Another core element of deterrence is the belief that an adversary has both the will and the capability to escalate measures if the other side does not change course. When Russia issued a litany of demands designed to highlight Ukraine and NATO’s vulnerabilities – from Ukraine’s status as a state to the overall European security architecture – its audience didn’t find its threats to be credible.

With the exception of the US, few believed that Russia would launch a full-scale invasion or persist with its threats against NATO and neutral states. Yet Russia did invade and has since issued veiled nuclear threats and even tested a new supersonic missile.

Similarly, Russian President Vladimir Putin did not take seriously French President Emmanuel Macron, German Chancellor Olaf Scholz, and other Western leaders when they expressed their intentions to support Ukraine. The Kremlin heard these statements, but it also heard several other leaders, including US President Joe Biden, say that they would not send troops to defend a non-NATO country. Russia thus decided to invade, only to be surprised by the scope and intensity of the West’s response.

For its part, Ukraine’s deterrence strategy was essentially to project an image of itself as a country that already belonged to the West. And though the Kremlin was unpersuaded, Russia clearly underestimated Ukrainian unity and the capability and competence of its army, even though it had been fighting Ukrainian forces since its incursions into the country in 2014.

Ukraine’s heroic self-defense reminds us that beyond the battlefield and business, beyond sanctions and institutions, there are ordinary people: the war is taking place among them, and they will decide its ultimate outcome. Though Ukrainians’ will to defend their lives, homes, and ideals has not yet deterred Russia’s leadership, there is strong evidence that it has deterred many Russian soldiers from fighting.

Looking ahead, Western deterrence must become a primary strategic objective and thus more comprehensive, including all the elements that matter. US Secretary of Defense Lloyd Austin took a step in this direction by announcing that one of America’s goals now is to “see Russia weakened to the degree that it can’t do the kinds of things that it has done in invading Ukraine.” And the $33 billion lend-lease bill that Biden signed on May 9 will further advance this goal.

But it’s not enough. Deterrence must be a popular aim that commands widespread public support. It also must be backed by other countries, because international cooperation is crucial for ensuring the security of smaller, vulnerable states. Achieving such broad-based support requires effective, inspirational leadership of the kind that Ukrainian President Volodymyr Zelensky has demonstrated. He has rallied not only the Ukrainian people but the entire Western world. Other leaders would do well to follow his example.

Finally, it is important to remember where deterrence fits in the broader context of globalization. Russia was emboldened by the economic interdependencies that it has cultivated, and it was empowered by its status as a permanent, veto-wielding member of the United Nations Security Council. Deterrence must include measures either to neutralize or contain both factors.

The war in Ukraine is the result of insufficient deterrence. Ultimately, there will be no peace without it.

## Hybrid War

### AT: hybrid war bad

#### Hybrid war obsession overblown – and cyber limited impact on hybrid war – small impact on warfighting and disinformation

Mueller, 2022

[John, Political Scientist at Ohio State University and a Senior Fellow at the Cato Institute, “The Cyber-Delusion: Digital Threats Are Manageable, Not Existential”, Foreign Affairs, 3/22/22, https://www.foreignaffairs.com/articles/russia-fsu/2022-03-22/cyber-delusion, accessed 7/4/22, GDI-cc]

Over the past decade, the global obsession with digital threats has taken various forms, with a particular focus on the potential military implications of emerging cyber-capabilities. To be sure, the military needs to worry about keeping its communications and command and control operations secure from hostile attackers. Any disruptions, however, are more likely to be instrumental or tactical than strategic.

Despite statements to the contrary, the U.S. military itself seems to have recognized this reality. When Panetta proclaimed in 2013 that cyber was “without question, the battlefield for the future,” political scientist Micah Zenko observed at the time that the Pentagon was spending less than one percent of its budget on cybersecurity, and an assessment from 2019 suggests it may be more like one-tenth of one percent. If those funds prove adequate for the challenge, it would be something of a bargain.

Cyber also supposedly enhances a state’s ability to carry out such ancient endeavors as espionage, propaganda dissemination, and sabotage. Analysts have even coined a new term, “hybrid warfare,” that usually includes these three enterprises—although, since the term does not include direct armed conflict, it might more plausibly be called “denatured warfare.” **Cyber’s contribution to these three areas**, however, **is relatively limited.**

Should invading hackers engage in digital espionage against the United States, for instance, they are likely to find that most of what they come across is already well known, and that much of the rest is not worth knowing in the first place. Wikileaks’ 2010 publication of thousands of classified U.S. government documents demonstrated the degree to which governments worldwide have fallen victim to over-classification. When Bill Keller, the editor in charge of poring over the documents at The New York Times, was asked whether the reporting team found anything they didn’t already know, he responded “no” without hesitation.

Much the same holds for concerns over the theft of intellectual property. Not only is this practice centuries old, but systematic stealing has often proved unwise because it distracts governments from homegrown innovation. Cyber-propaganda efforts, in turn, are more likely to increase the overall amount of available information and disinformation—an age-old problem in warfare—than to provide a decisive advantage.

## Nuclear forces/deterrent

#### See also signaling answers and offensive cyber operations answers

### AT: NATO nuclear force deters Russia

#### US nuclear umbrella doesn’t deter Russia – no fear of reprisal

**Hooker**, Non-Resident Senior Fellow at the Atlantic Council, **2022**

(Jr R.D., "The State of NATO: An American View," Survival, Vol. 64, no. 3, pg. 103-113, 2022, Taylor & Francis, accessed 6/30/2022, gdi-tmur)

For much of the Cold War, NATO relied on the US nuclear deterrent to offset its conventional inferiority. Many continue to believe that the American nuclear umbrella will ensure deterrence. But Russia maintains powerful tactical nuclear munitions that can be delivered from a variety of air-, sea- and ground-based platforms. Its nuclear forces are rehearsed and ready, backed up by an intimidating ‘escalate to de-escalate’ nuclear doctrine.21 It is doubtful that Putin fears a nuclear response in a limited conventional incursion into NATO territory. In any case, Russia’s nuclear options below the strategic threshold give it clear advantages in this scenario.

## Russia

### Squo solves Russia threat – troops

#### SQ solves – NATO increased response force to counter Russia

**CENFE, 2022**

[CE Noticias Financieras English, “NATO to launch largest military reinforcement in Eastern Europe against Russian threat”, CE Noticias Financieras English, June 27, 2022, Lexis, accessed July 7, 2022, GDI-LL]

NATO is not at war, but it is rapidly preparing for it. Since Russia invaded Ukraine, the military alliance has multiplied its resources in member countries bordering the aggressor or in close proximity. And it is not going to stop. "We are going to raise our forces in the east from battalion to brigade level," announced the organization's secretary general, Jens Stoltenberg, at the press conference ahead of the Madrid Summit, which takes place between Tuesday and Thursday. This leap opens the door to doubling deployments. The current battle groups are made up of between 1,000 and 1,600 soldiers. A brigade could be at least twice that number. The Norwegian added that the heads of state and government will agree to increase NATO's rapid response force in case of conflict to "more than 300,000″ soldiers, i.e. more than eight times its current number. "The goal is to send the message that we are ready to protect and defend every inch of allied territory," the Norwegian has warned, composing in his own way the famous Latin phrase Si vis pacem, para bellum (if you want peace, prepare for war).

#### SQ solves – NATO increasing troop presence to demonstrate preparation to protect from Russia

**CENFE, 2022**

[CE Noticias Financieras English, “NATO to launch largest military reinforcement in Eastern Europe against Russian threat”, CE Noticias Financieras English, June 27, 2022, Lexis, accessed July 7, 2022, GDI-LL]

There is little more palpable evidence of what the invasion of Ukraine has meant in the geostrategic sphere - and its prolegomenon of the annexation of Crimea in 2014 - than the Strategic Concept that NATO approved 12 years ago. In that document, which sets out the alliance's strategy for the next decade, Russia appeared as a "partner" of the Alliance. In the one to be approved in Madrid, the aggressive neighbor to the far east of Europe will be defined as "the most significant and direct threat to security," Stoltenberg explained.

To deal with that threat, the organization, with strong U.S. leadership, is prepared to take steps unthinkable last January, just weeks before Putin's war in Ukraine began. Now the organization has deployed in the eastern countries (Estonia, Latvia, Lithuania, Poland, Slovakia, Hungary, Romania and Bulgaria) most of the 40,000 troops it has under its command, some 25,000 soldiers, according to its own figures. And Stoltenberg has announced that this deployment will go further by announcing this move from battalions to brigades.

"The increased presence from battalions to brigades will be in some countries. This does not apply to all. There are different needs for each country," the secretary general clarified, after pointing out that between February and now, NATO has already doubled the number of battalions in the east, from four to eight.

Most of Stoltenberg's appearance was aimed at putting on the table the effort that NATO is prepared to make to protect itself from the former partner that has now become an enemy. And that effort involves putting more money on the table. Because the war and its preparations, even if it is only to scare it away, require many millions of dollars and euros. Here he has warned that the commitment remains that reached in 2014 at the Wales Summit: to raise to 2% of GDP the spending of the 30 allied States: "It is a floor, not a ceiling". In other words, it is the minimum spending required by the organization.

### Squo solves cyber – Ukraine proves

#### Russia ineptness and Ukraine resiliency undermine effective cyber – multiple examples

**Srivastava et al.**, CYBERSECURITY CORRESPONDENT, **2022**

(Mehul “The secret US mission to bolster Ukraine’s cyber defences ahead of Russia’s invasion” Financial Times Mar 9, 2022 proquest accessed 6/28/2022 gdi-tmur)

So far, experts who have watched the Russian cyber assaults have been confused at their lack of success, as well as the lower tempo, intensity and sophistication of what Russian-government hackers are known to be capable of.

Ukrainian defences have proved resilient, said one European official who was briefed this week by the Americans at a Nato meeting, and Russian offences have proved mediocre. He said the reason was that, so far, Russia has held back its elite corps in the cyber arena, much as it has on the battlefield, perhaps by underestimating the Ukrainians.

One example, he said, was the fact that instead of communicating solely through encrypted military-grade phones, Russian commanders are sometimes piggybacking on Ukrainian cell phone networks to communicate, at times simply by using their Russian cell phones.

“The Ukrainians love it — there is so much data in simply watching these phones, whether or not they are using encrypted apps,” he said.

The Ukrainians then block Russian phones from their local networks at key moments, further jamming their communications. “Then you suddenly see Russian soldiers grabbing cell phones off Ukrainians on the street, raiding repair shops for sims,” he said. “This is not sophisticated stuff. It’s quite puzzling.”

### AT: Russia impact – war escalates

#### Past assessments of Russia’s military power are false – Russian forces are weak and don’t present a substantial threat – Ukraine invasion proves

Gramer and Mackinnon, 2022

[Robbie, diplomacy and national security reporter at Foreign Policy, and Amy, national security and intelligence reporter at Foreign Policy, "NATO Allies Are Rethinking Russia’s Suppossed Military Prowess", Foreign Policy, 6/7/22, https://foreignpolicy.com/2022/06/07/ukraine-nato-allies-rethinking-russia-military-prowess/?utm\_source=PostUp&utm\_medium=email&utm\_campaign=Editors%20Picks%20OC&utm\_term=43213&tpcc=Editors%20Picks%20OC, accessed 7/4/22, GDI-cc]

During his decade and a half at the Pentagon, Christopher Skaluba read countless reports and assessments on the Russian military and how it squared up against NATO forces. Now that he has left and has watched Russia’s invasion of Ukraine falter for months, he has a new message for defense planners: “Every single one of those assessments that I’ve read for the last decade and more have been wrong.”

Across NATO, defense planners are reassessing Moscow’s military might in their contingency plans in the unlikely event of a conventional war between the alliance and Russia, according to multiple current and former U.S. and European defense officials. The reassessments come after Moscow’s embarrassing military setbacks in Ukraine, as well as the Kremlin’s willingness to launch a full-fledged military invasion in the first place.

There are two major assumptions that defense planners in major NATO capitals got wrong for years, former NATO Secretary-General Anders Fogh Rasmussen said in an interview with Foreign Policy. First, Rasmussen said, “we have overestimated the strength of the Russian military.

Despite huge investments in military equipment and the reopening of old Soviet bases, we have seen a very weak Russian military.” “The other miscalculation is we have underestimated the brutality and the ambitions of President [Vladimir] Putin,” Rasmussen added.

Now, in capitals in Europe and North America, wonks in defense ministries are dusting off years-old assessments of the Russian military’s fighting prowess and starting to question long-held assumptions on what a conventional war between NATO members and Russia would look like.

“Whether it was morale or communications or lack of preparedness, there’s a bunch of factors that have added up to something that you just wouldn’t expect to see from an advanced military,” Skaluba said of the Russian forces, “even if the initial conditions or assumptions under which they went in [to Ukraine] were invalidated.”

## Space capabilities

#### Supplement will have additional space answers

## Supply Chain

### Non-unique – sustained economic problems now

#### No shock from hack – economic conditions here to stay

**Tan, 2022**

[Su-Lin, “Global recession? Not yet, economists say — but brace for high prices, low growth” CNBC, MAY 30 2022, [https://www.cnbc.com/2022/05/30/no-global-recession-yet-but-brace-for-stagflation-economists-say.html accessed 7/7/22](https://www.cnbc.com/2022/05/30/no-global-recession-yet-but-brace-for-stagflation-economists-say.html%20accessed%207/7/22) GDI-TM]

A global recession is not imminent, but brace for rising costs and slower growth, economists say. “There will be no sudden ‘after’ of stagflation,” said Simon Baptist, global chief economist at the Economist Intelligence Unit, referring to a surprise recession after a period of stagflation. As the war in Ukraine and pandemic disruptions continue to wreak havoc on supply chains, stagflation — marked by low growth and high inflation — will stick around “for at least the next 12 months,” Baptist told CNBC last week. “Commodity prices will start to ease from next quarter, but will remain permanently higher than before the war in Ukraine for the simple reason that Russian supplies of many commodities will be permanently reduced,” he added. The pandemic as well as the war in Ukraine have stifled supply of commodities and goods and upended efficient distribution through global supply chains, forcing up prices of everyday goods such as fuel and food. But, while higher prices will cause pain for households, growth in many parts of the world, while slow, is still ticking over and job markets have not collapsed. Unemployment levels across many economies have reached their lowest in decades.

#### No recession likely

**Tan, 2022**

[Su-Lin, “Global recession? Not yet, economists say — but brace for high prices, low growth” CNBC, MAY 30 2022, [https://www.cnbc.com/2022/05/30/no-global-recession-yet-but-brace-for-stagflation-economists-say.html accessed 7/7/22](https://www.cnbc.com/2022/05/30/no-global-recession-yet-but-brace-for-stagflation-economists-say.html%20accessed%207/7/22) GDI-TM]

So, consumers — while wary of a repeat of the last global recession brought on by the U.S. subprime crisis over 10 years ago — need not start preparing for a recession. “For almost all economies of Asia, a recession is fairly unlikely, if we’re talking about successive periods of negative GDP,” Baptist told CNBC’s Street Signs on Thursday. Even if the global economy is at risk of a recession, many consumers have ample savings and have stocked up on household durables, the economist said. “So to an extent, it won’t feel as bad as the immediate numbers look,” he said. AMP Capital chief economist Shane Oliver doesn’t see the recession writing on the wall either, at least not for another 18 months.

### Economy slow down now

#### Inflation and supply disruptions persist – energy, war in Ukraine

**Guenette, 2022**

[Justin, “How sharp will be the global slowdown?” Brookings, July 1, 2022 <https://www.brookings.edu/blog/future-development/2022/07/01/how-sharp-will-be-the-global-slowdown/> Accessed 7/7/22 GDI-TM]

The war in Ukraine has caused significant supply disruptions and higher price volatility across several commodities, including energy, food, and fertilizers. There are many possible triggers for further upward movements in energy prices. These are all driven by the Russian invasion of Ukraine and could include an immediate ban by Russia on all energy exports to EU members, additional G-7 sanctions targeting shipping companies, and the possibility of secondary sanctions on third parties purchasing Russian energy supplies. In a scenario of additional major disruptions to energy markets centered around Europe, the prices of natural gas, oil, and coal could spike in the third quarter of 2022 and remain elevated over the remainder of the scenario horizon, reflecting both precautionary buying and lower global supplies. Growth would slow sharply in advanced economies—particularly in the euro area—while EMDEs would face notable headwinds from higher energy prices and weaker foreign demand. On net, global growth could be reduced by 0.5 percentage point in 2022 and a further 0.7 percentage point in 2023.

# Solvency Answers

## Arms Control – Cyber

### 1NC – International cyber arms control fails

#### Cyber arms control agreement fail – laundry list

Benincasa, 2021

[Eugenio, WSD-Handa Resident Fellow at Pacific Forum in Honolulu, "The Case for Cyber ‘Disarmament’ in the European Union", Italian Journal of International Affairs, Vol. 56, Issue 1, 2021, LexisNexis, accessed 7/2/22, GDI-cc]

The last two decades of multilateral dialogue on state behaviour in cyberspace have thus  been unable to establish clear rules and standards for cyber operations, raising concern  about an arms race in cyberspace. Influential experts such as Richard Clarke, former  Special Advisor on cybersecurity to President George W. Bush, have explicitly called for  creation of a cyber arms control regime (Bronk and Wallach 2013). In 2015, The  New York Times (2015) supported the idea of an arms control treaty in cyberspace,  stating that “the best way forward is to accelerate international efforts to negotiate limits on the cyber arms race, akin to the arms-control treaties of the Cold War”. Nonetheless,  this possibility will have to be assessed in light of the inherently unique nature of the  cyber domain.

Most of the multilateral arms control agreements were negotiated with the aim of  limiting specific type of arms and their geographical proliferation, in some cases leading  to their total and effective ban. After the end of the Cold War and the waning of the  bipolar system, it soon became clear that arms control had to be implemented in other  areas besides nuclear power, such as biological and chemical weapons. To establish  universal frameworks to reduce such threats, consensus among major global players  was deemed essential. In the context of cyberspace, today’s global players differ not only  in their strategic interests, but also in their conceptual frameworks of what constitutes  cyberspace. While there is no universal definition of a cyber weapon, it can be described  as a computer program designed to compromise the integrity or availability of data in an  enemy’s ICT system for military purposes (Perkovich and Levite 2017). Importantly,  weaponry and non-weaponry malicious software look very similar in terms of their  technical components. They require both an ‘exploit’ and a ‘payload’ in order to function.  An exploit is a program or a piece of code that, while not malicious in itself, takes  advantage of a security flaw in an application or system – a so-called ‘vulnerability’ – that  allows an intruder to access a network remotely (Herr 2014). A software vulnerability  that is previously unknown is called ‘zero day’, due to the fact that the vendor has literally  zero days to fix it. The payload contains the actual attack component, that is, the  malicious code targeting and tailored to a specific ICT system with the aim of causing  damage. The effects of the payload can range from surveillance and data exfiltration to  actual physical damage. Zero days can be thought of as the ‘ammunition’ of cyber  weapons and the payload as their ‘trigger’.

Bringing all relevant parties together – including non-state actors – to agree on a shared conceptual framework of cyberspace for the purpose of arms control does not seem to be a realistic or sustainable objective for the time being. Additionally, even if the above-mentioned conceptual disparities were to be solved, a cyber arms control regime based on traditional arms control treaties would be hard to enforce because of some inherent characteristics of cyberspace and their implications for the purposes of arms control. More specifically:

● Assessing relative strength: In order to negotiate an agreement that can promote stability by effectively imposing restrictions upon the development, production, stockpiling and usage of certain types of weapons, states need to have an under- standing of each other’s relative strength. As explained by Erica Borghard and Shawn Lonergan (2018), “for conventional munitions, nuclear weapons, or even chemical ordinances, warheads or pounds of a virulent gas that a state possesses can be counted, allowing others to assess comparative strength. The same cannot be said for assessing relative strength in cyberspace”. Virtual weapons cannot be counted and, once produced, can be easily duplicated and transmitted to other locations at no cost via different means, such as email, websites, instant messaging, peer-to-peer sharing, etc (Denning 2001). “To copy a cyber weapon, all you have to do is see it, because the weapon itself is made of information” (Hitchens 2019). These circum- stances make cyber strength assessment unfeasible. In contrast, the technical skills of cyber threat actors may be easier to measure than virtual weapons (Borghard and Lonergan 2018), but negotiating and enforcing an agreement imposing skill-based restrictions would add other complexities. Barring the skills used to craft cyber weapons would be equivalent to prohibiting “how-to” information, or “making advanced mathematics illegal” (Libicki 2009, 199): in other words, impossible. The impact of such an approach would not be desirable either, given that the skills needed to craft offensive cyber tools are also used by law-abiding actors to build defences and by intelligence agencies to conduct cyber espionage, an activity in which everyone has a stake (Ibid.).

● Verification of compliance: The mutual verification mechanisms needed to ensure that all parties abide by the agreed terms is quite an intrusive process, and states are wary of sharing sensitive national security information with external actors – especially adver- saries. Within a cyber arms control framework, compliance verification would require states to have access to each other’s networks – public, private and classified – and scan them to find potential threats (Denning 2001). This is an unimaginable scenario for several reasons. Not only would “such access [. . .] provide an external party with critical information about vulnerabilities and potential exploits, and potentially violate the agreement it is attempting to enforce”, it would also raise questions about the inherent differences between a monitoring compliance process and espionage activity (Borghard and Lonergan 2018). China and Russia have already dismissed the possibility of accepting the more limited level of intrusion proposed by the Budapest Convention for cybercrime cooperation. It is therefore unthinkable that they, or any other state, would agree to the systematic and routine level of intrusion into their systems that would be required by a potential cyber arms control regime. In addition, even if states were to agree to a similar approach, unearthing hidden virtual threats would be an onerous task due to the vastness and complexity of network systems, and to the fact that cyber weapons can be duplicated instantaneously and sent to other locations at no cost (Denning 2001).

● Enforcement: Charging states with violating arms control treaty obligations can be a challenging endeavour in the cyber domain. In the aftermath of a cyberattack, offenders are often difficult to identify and prosecute due to the problem of attribution and the lack of unfettered access to individual state jurisdictions in order to investigate transnational cyber offences. States’ disagreement over the reach and scope of extra- territorial searches into their networks for investigative purposes was one of the main objections to the cybercrime cooperation model put forward by the Budapest Convention, and its perceived violation of the principle of state sovereignty remains one of the main ideological differences among major global players. As for attribution, research has shown that the lack of effective attribution can contribute to freeing parties of their responsibilities if they think they cannot be caught, thus not deterring non-compliance (Barbieri et al. 2018). In fact, even if technical attribution – the identification and localisation of the source node which initiated the attack – can be achieved, human attribution – the identification of the actual actor responsible for the cyberattack – can be much harder, given the complexity of a group’s affiliation or involvement in cyber operations. In addition, attribution has to be communicated effectively to convince the other parties to the treaty that a violation has actually taken place, but states are often reluctant to show proof for fear of disclosing classified forensic methods and sources (Nye 2016/17). Last but not least, these tasks have to be carried out in a timely manner after a cyberattack. Yet, especially in the case of attacks involving corruption as opposed to disruption, “there may be a significant time lag between when a derogation occurs and when it is actually observed. Thus, the deterrent effect of a response is likely to be diluted by the simple passage of time” (Borghard and Lonergan 2018).

● Trust: Arms control treaties can be helpful in slowing down a dangerous arms race between adversaries and building the foundations for enhanced trust. Nevertheless, US relations with China and Russia are at an all-time low, and are characterised by deep mistrust and rising tensions that are unlikely to abate in the foreseeable future. Moscow’s interference in the 2016 and 2020 US presidential elections (Goldman et al. 2020), as well as the annexation of Crimea in 2014 and its involvement in Syria and Venezuela in stark opposition to US interests have shaped adversarial dynamics between the two countries (US Department of State 2020). The US-China relationship has deteriorated even more dramatically as the two states have been dismantling decades of political, economic and social cooperation, heading towards a new era of confrontation driven by Beijing’s increasing ambition to become the next hegemonic power (Wong and Myers 2020). In the context of cyberspace, these geopolitical knots translate into the different ideologies and strategic interests analysed previously, making cooperation and the building of trust increasingly less likely.

### Extension – no international agreement

#### No cyber arms control agreement – too many obstacles

Benincasa, 2021

[Eugenio, WSD-Handa Resident Fellow at Pacific Forum in Honolulu, "The Case for Cyber ‘Disarmament’ in the European Union", Italian Journal of International Affairs, Vol. 56, Issue 1, 2021, LexisNexis, accessed 7/2/22, GDI-cc]

The entanglement of geopolitical and technical difficulties makes it hard to believe that a cyber arms control agreement will be achieved in the foreseeable future. This does not mean that it will never happen: states may eventually reconcile their differences, and technical problems related to attribution may finally be solved. Relevant organisations such as RAND, the Atlantic Council and the Microsoft Corporation have proposed different models for the creation of an international attribution organisation to meet these challenges (Mueller 2017). However, no sweeping change in cybersecurity global governance should be expected to take place any time soon, including the negotiation of a cyber arms control agreement. Nevertheless, while the concept of arms control itself should not be abandoned, it could be looked at from a different perspective, stepping out of the box created by Cold War frame- works. In addressing this issue, Martin Libicki (2009, 199) has asserted that “a good deal depends on what one means by arms control. If the model were to be something like the treaties signed between the United States-NATO and the Soviet Union-Warsaw Pact, which limited certain classes of weapons and banned others, there is little basis for hope”.

## Cyber effects

### Cyber effects fail

#### Operational integration of cyber effect limited – multiple factors including difficulty reusing exploits, secrecy challenges in hot conflict, info on critical military networks – can’t solve Russia through NATO request effect model

\*ev also says to maintain advantage of cyber arsenal needs labor foundation highly trained

Jacobsen, 2022

[Jeppe, PhD candidate Danish Institute for International Studies and the University of Southern Denmark and former coordinator of Denmark’s cyber diplomacy in European Union and NATO, "Cyber Offense in NATO: challenges and opportunities", International Affairs, Vol. 97, Issue 3, May 2021, https://academic.oup.com/ia/article-abstract/97/3/703/6205395, accessed 7/1/22, GDI-cc]

The abovementioned incidents have led cyber-conflict scholars to point to several technical and practical difficulties in the operational integration of cyber effects.29 In the interviews and background conversations that contributed to this study, three of these difficulties were continuously reiterated when discussing successful integration of cyber effects into NATO operational planning: the temporal dimen- sion of developing exploits; the assessment of battle damage; and the problem of confliction.

Developing exploits—a matter of time

One of the characteristics of cyber attacks that receives most attention is the fact that they hit suddenly and without warning.30 While this is often the case, the central question for operational integration is not the speed at which they hit their target, but the speed with which the tools and techniques that exploit IT vulnerabilities in order to deliver cyber effects can be developed. Like conven- tional weapons, the cyber tools—the exploits or cyber weapons—take time to develop. However, an exploit is often harder to reuse than a conventional weapon, as it is more dependent on a meticulous analysis and target preparation—in this case, specifically, the target’s IT infrastructure. Without knowing the adversary’s IT systems and its vulnerabilities better than the adversary itself, meaningful cyber weapons are impossible to develop.

The fact that knowledge about the target is linked not only to the deployment of a weapon but also to its development influences the extent to which it can be used and reused. Stuxnet, for example, required years of development, testing and perfecting before it could deliver the intended effect on the Iranian centrifuges. Despite the techniques used in the Stuxnet malware having been found in other malware,31 Stuxnet lost its ability to destroy the centrifuges when it was discov- ered and the IT vulnerabilities that enabled it were patched. Importantly, part of the complexity of Stuxnet relates to the US–Israeli intention to keep the effect secret. In a hot conflict, secrecy in terms of the effect is often less important, and thus the development and deployment of cyber effects do not necessarily have to be as complex and time-consuming.

This observation does not necessarily change the fact that the development of exploits often has to precede the military confrontation in which they are intended to be used. NATO states that want to deliver cyber effects in NATO operations must try to gain access to Russia’s or other potential adversaries’ critical military networks to identify and exploit IT vulnerabilities. As several informants empha- sized, if states wait for a conflict to escalate before they begin the development of exploits, it is most likely to be already too late.32

The alternative to penetrating adversary networks in peacetime is for states to rely on the exploitation of vulnerabilities in as many commercial off-the-shelf products as possible. This can be done, for example, by purchasing exploits from private companies offering this service, in the hope that it will then be possible to quickly create an overview of the enemy’s IT infrastructure and adapt the exploits to this environment when a conflict escalates. The latter approach is more likely to succeed against adversaries with low network security, which does not apply in the case of Russia, or in contexts where less sophisticated and less closely targeted cyber effects are required.

Whether member states develop sophisticated exploits for future targeted effects or stockpile well-known exploits to cause more minor effects, they cannot—as several informants indicated—be certain that they will be able to deliver the cyber effect at the specific time it is requested by CYOC. This is because the IT vulnerabilities upon which exploits depend might not exist for ever. Cyberspace is a dynamic environment: vulnerabilities are patched, systems are updated or replaced and bad IT security practices are identified and improved. This means that exploits are temporary in nature and cannot be stored for later use.33 States must constantly ensure that the exploits still work, which requires minor adjust- ments when updates take place. As a consequence, the larger the military ‘cyber arsenal’, the more technically skilled human resources are needed for its mainte- nance. In the current labour market, where recruitment and retention of a cyber workforce is difficult, extensive investment is required for states to be able to stand ready with cyber effects available when requested.

In short**, if a state is to offer a cyber effect in a NATO operation, then the state is likely to have to be able, first, to predict what Russian IT systems it is going to target months or years in advance, and second, to marshal the necessary resources to develop and maintain a large array of exploits that can be used against these systems. Even if this is successfully done, the state still faces difficulty in ensuring that an effect is delivered as promised.**

#### Cyber effects focus won’t deter Russia – invasion risk because of other NATO credibility issues

Jacobsen, 2022

[Jeppe, PhD candidate Danish Institute for International Studies and the University of Southern Denmark and former coordinator of Denmark’s cyber diplomacy in European Union and NATO, "Cyber Offense in NATO: challenges and opportunities", International Affairs, Vol. 97, Issue 3, May 2021, https://academic.oup.com/ia/article-abstract/97/3/703/6205395, accessed 7/1/22, GDI-cc]

NATO’s founding purpose was to maintain a sufficient military strength to deter aggression and attempts at coercion, to prepare for the eventuality of deterrence failing, and to ensure stability among European powers.51 During the Cold War, the debates over NATO deterrence posture largely centred on the role of nuclear weapons, and specifically whether the United States would retaliate with these weapons in the event of a Soviet conventional attack against allied states.52 In short, NATO deterrence was about credibly extending the US nuclear (as well as conventional force) deterrence to allies to discourage a Soviet military offensive into eastern Europe.

While NATO and its member states adapted to the new security environ- ment after the end of the Cold War by scaling down the military investments and presence in eastern Europe and by focusing more on crisis management,53 much of the Cold War deterrence language returned when the Russian–Ukrai- nian conflict broke out in 2014.54 What needs to be deterred today, much of the literature agrees, is not only a full-scale military invasion but to a larger extent the use and support of pro-Russian militant separatists who are willing to apply insurgency tactics in NATO’s post-Soviet member states.55 As a result, the allies’ military investments have been increasing again,56 a number of initiatives such as the Enhanced Forward Presence in the Baltic States and Poland have been introduced,57 and the discussions—and disagreements—on the nuclear deterrence (of non-nuclear threats) have re-emerged.58 Such responses are often presented as a renewed attempt by NATO to reassert its deterrence and assurance posture by signalling strength, preparedness and willingness to punish ‘bad’ behaviour.59 At first sight, the introduction of CYOC seems to add to these deterrence efforts. NATO added an offensive cyber option to reinforce its ability to impose costs sufficient to dissuade adversaries from acting aggressively. On closer exami- nation, however, it is not self-evident that requesting member states’ delivery of offensive cyber effects in NATO operations constitutes a necessary or even a substantial addition to credibly signalling the ability and willingness to punish an adversary. NATO’s conventional capabilities are clearly already far superior to Russia’s—with or without fully integrated cyber effects. Thus, a deterrence failure, resulting for example in a scenario in one of the Baltic states similar to that which occurred in eastern Ukraine, will not be the result of NATO’s lack of available cyber tools in its military toolbox; rather, if the Russian leadership were to consider it in its interest to pursue such a scenario, it would mean that Russia’s decision-makers did not believe in the credibility of NATO’s article 5 or in NATO’s ability to mobilize its forces. **The capacity to integrate cyber effects would do nothing to change that.**

#### No NATO integration of cyber effects – multiple factors means won’t use in conflict if other capabilities available

Jacobsen, 2022

[Jeppe, PhD candidate Danish Institute for International Studies and the University of Southern Denmark and former coordinator of Denmark’s cyber diplomacy in European Union and NATO, "Cyber Offense in NATO: challenges and opportunities", International Affairs, Vol. 97, Issue 3, May 2021, https://academic.oup.com/ia/article-abstract/97/3/703/6205395, accessed 7/1/22, GDI-cc]

This section has pointed to three characteristics about cyberspace that limit the integration of cyber effects in NATO operations. In a complex and constantly changing cyberspace, it continues to be difficult to develop and maintain sophis- ticated exploits for targeted cyber effects. This is especially the case if the cyber effects are requested for a specific time and place in order to guarantee operational success, and if they simultaneously have to be verifiable and conform to interna- tional legal principles. Neither the member states, which face an internal dilemma between attack, intelligence collection and defence in cyberspace, nor the NATO commander, who will prefer to control the capabilities used, are likely to feel suffi- ciently confident about the targeted or highly integrated cyber effects to choose that option if other capabilities are available.

#### Multiple incentives for NATO states to resist request based model to contribute to cyber effects

Jacobsen, 2022

[Jeppe, PhD candidate Danish Institute for International Studies and the University of Southern Denmark and former coordinator of Denmark’s cyber diplomacy in European Union and NATO, "Cyber Offense in NATO: challenges and opportunities", International Affairs, Vol. 97, Issue 3, May 2021, https://academic.oup.com/ia/article-abstract/97/3/703/6205395, accessed 7/1/22, GDI-cc]

Confliction—the issue of secrecy

The third challenge to the integration of cyber effects in NATO operations relates to a well-known military concept, deconfliction. The coordination by allies and military units of their efforts to avoid confliction, between for example an air operation and a special forces operation in the same area, is a central element in every military campaign. Deconfliction is all about openness and communica- tion between allied partners. But in cyberspace, deconfliction comes with several difficulties. At the core of these difficulties is the fact that **the tools and techniques that produce cyber effects—which are often also used and heavily depended on for intelligence collection—are developed in secret and must stay secret until the effect is achieved.** If the IT vulnerabilities and exploits are known, vendors or adversaries can fix or replace the software and thereby render the effect impossible to achieve.39 **In an alliance not known for sufficient mutual trust among members to share intelligence,40 there is little indication that allies will become more open about the cyber tools and techniques they currently have at their disposal.** **The request-based model is the result of that lack of trust**. **And the unwillingness to share cyber intelligence seriously challenges NATO’s ambition to use CYOC to facilitate information-sharing to increase situational awareness and thereby achieve the ‘cyber readiness’ and ‘cyber resiliency’ that NATO Deputy Secretary-General Mircea Geoană hopes to attain**.41

Furthermore, lack of coordination and discussion about the use of military cyber capabilities, both internally in each state and among allies, can have negative implications for intelligence activities and general network security. A conventional military decision to deliver cyber effects is rarely concerned with maintaining access and staying secret after an effect is achieved. Even though it is customary to try to obscure the vulnerabilities that are being exploited, it is difficult to ensure that those operating the targeted system or third-party network analysts do not identify and fix the vulnerabilities in, for example, commercial products used all over the world. Thus, military plans to engage other state entities need to weigh the benefit of delivering cyber effects against the risk of losing intel- ligence capacity, as well as the risk that other actors (allies, corporations, adver- saries, criminals, etc.) will use the same exploits against oneself. In other words, there is a conflict of interest between attack, intelligence collection and internal defence in each NATO member state.42 The desire of the US Cyber Command to become more independent from the National Security Agency (NSA) is precisely an attempt to gain a stronger voice when the US government assesses whether a vulnerability should be disclosed to vendors, retained for intelligence purposes or used to deliver ‘loud’ cyber effects.43

The risk of confliction among allies arises from the fact that a similar assessment procedure does not exist across NATO. As conversations with several national representatives at the CDC reveal, such a procedure is unlikely to be agreed upon owing to the different perspectives on offence, defence and espionage in cyberspace currently prevailing among member states.44 If the Netherlands, for example, offers to deliver a ‘loud’ cyber effect in a NATO operation, British or American intelligence operations could end up being disturbed because they rely on the same vulnerabilities which—when used in military operations—risk being exposed and subsequently fixed.45 When deploying ‘loud’ cyber effects, malicious actors such as criminals are also given the opportunity to identify and exploit the same vulnerabilities in unpatched systems in allied countries. The ransomware incidents known as WannaCry and NotPetya are examples of the damage that can emerge from government exploits becoming publicly available—even though the specific vulnerabilities were already patched by Microsoft and updates released to supported systems.46

In short, there is a dilemma both internally, between intelligence agencies and the military, and externally, between allies. While it is difficult to do much about the latter, the internal power dynamics in most states, with the intelligence agencies as the primary cyber actors, are likely to limit the willingness of most states to deliver military cyber effects—whether offensive or defensive—when CYOC makes requests. They also limit the willingness to share cyber threat infor- mation across the alliance through CYOC.

#### NATO country cyber effects limited effectiveness – laundry list of reasons undermines effectiveness versus Russia

Jacobsen, 2022

[Jeppe, PhD candidate Danish Institute for International Studies and the University of Southern Denmark and former coordinator of Denmark’s cyber diplomacy in European Union and NATO, "Cyber Offense in NATO: challenges and opportunities", International Affairs, Vol. 97, Issue 3, May 2021, https://academic.oup.com/ia/article-abstract/97/3/703/6205395, accessed 7/1/22, GDI-cc]

How likely is it that the requested cyber effect will be delivered? The answer to this question is not clear, in respect of either its preparation or its execution. This is not only because IT vulnerabilities are constantly discovered and patched; it is also because of the difficulty of assessing the effects and possible side-effects of an exploit when navigating and analysing complex IT infrastructures. In other words, reconnaissance is difficult in cyberspace, and so is the containment of effects. The Russian attempt to use ransomware aimed at disrupting critical Ukrainian infrastructure in 2017, for example, succeeded—but simultaneously encrypted computers globally, causing substantial economic damage to multina- tional businesses such as Maersk and FedEx.34

Collateral damage and unintended consequences are serious issues for NATO. The alliance takes pride in its adherence to the principles laid out in international law, such as proportionality and discrimination, as former NATO Deputy Assis- tant Secretary-General Jamie Shea has emphasized.35 Thus, disruptions of servers with huge negative implications for civilians, or the use of generic cyber tools that risk spreading their effects far and wide, are most likely not going to be considered for use in NATO operations. Indeed, one of the main challenges to US efforts to disrupt servers in working against ISIS was finding ways to ensure that civilians were not hit by their cyber effects.36

Another aspect of the difficulty of assessing the cyber effect relates to adver- saries’ cyber defence efforts. For the more sophisticated players in cyberspace, cyber defence has developed into more than simply patching, clearing and updating systems. Cyber defence is also increasingly about following an intruder’s activity in one’s own network and creating ‘honeypots’ or ‘honeynets’; or about following data traffic back to the intruder’s network. In short, cyber defence is also about deception and active defence.37 This approach to cyber defence offers valuable insights into the intruder’s techniques and strategies; but the mere knowledge that deception is becoming a predominant defensive strategy also introduces doubts into the intruder’s assessment of possible effects.

Consequently, as Russia is considered a peer competitor with considerable cyber-defensive capacities, one informant expressed scepticism about the extent to which smaller member states are confident in their ability to deliver a cyber effect when it is requested by NATO.38 This is especially the case if operational success depends on a specific effect. Even if a state has developed the appropriate exploit, it must also be able to verify that the effect is achieved and ensure that the effect is contained to minimize collateral damage. And even if a state is confident about its current ability to contain and verify an effect, it must also be confident that it can deliver, verify and contain the effect at the specific time in the future when CYOC requests it.

The process of integration is further complicated by the fact that NATO must be willing to hand over to contributing states the responsibility for making battle damage assessments and collateral damage estimations. As the following subsec- tion shows, states are generally unwilling to share classified information about exploits. Hence, the delegated NATO commander is unlikely to receive much useful information about how cyber effects are delivered before a decision about their deployment must be taken. As commanders would prefer to have control over the capabilities used, member-state cyber effects are likely choices of method only if alternative, conventional effects are unavailable.

The challenges associated with assessing cyber effects are naturally most signifi- cant in relation to those effects that enable other kinetic effects that are necessary to achieve operational success. For cyber effects that seek to maintain a persistent annoyance of Russian networks, these challenges are less of an issue. If the aim is to create confusion and drain resources by targeting networks and operations that are otherwise difficult and expensive to disrupt using conventional means, then cyber effects can support strategic goals without causing irreversible damage to civilians. As I will conclude at the end of this section, such a change demands an adaptation of the way in which CYOC operates.

### Request based model fails

#### No internal link – no consensus definition of cyber weapon and offense in context of NATO even with request based model of cooperation

Jacobsen, 2022

[Jeppe, PhD candidate Danish Institute for International Studies and the University of Southern Denmark and former coordinator of Denmark’s cyber diplomacy in European Union and NATO, "Cyber Offense in NATO: challenges and opportunities", International Affairs, Vol. 97, Issue 3, May 2021, https://academic.oup.com/ia/article-abstract/97/3/703/6205395, accessed 7/1/22, GDI-cc]

During the past decade and a half there has been a rapid increase in the scholarly attention paid to various aspects of cyber conflict. Many debates have centred on the legally and strategically important task of providing more clarity to what we mean when we use concepts such as cyberspace, cyberwar, cyber warfare and cyber attacks. Despite the fact that most scholars now agree that it is unproduc- tive to characterize every cyber intrusion—large or small—as a cyberwar, acts of cyber warfare or cyber attacks,10 these concepts continue to be used in popular and academic discourse to describe a wide range of phenomena.11 Scholars have there- fore tried to define and nuance the cyber terminology by adding more concepts, such as ‘cyber weapons’ and ‘offensive cyber operations’ to focus attention on more military matters.12 Even these attempts have faced difficulties, however. There is as yet, for example, no consensus on what type of disruption or destruction (physical, digital or cognitive) a cyber weapon needs to be capable of creating to count as a weapon.13 And using the term ‘offensive’ has just spurred more debate on the blurred distinctions between offence and (active) defence.1

The latest suggestion for the appropriate terminology to use when speaking about the more aggressive military use of cyberspace is ‘military cyber effects’—a term that has become especially popular in the context of NATO operations. Here, the only way for NATO to move beyond simply protecting its own networks in its military operations has been to ask states to deliver cyber effects. As several conversations with both national and NATO representatives revealed, NATO’s request-based model is a compromise; it is the only possible solution to the fact that member states are reluctant to hand over specific knowledge about the cyber tools and techniques they use when delivering cyber effects to an allied commander.15 Conceptually, the term ‘cyber effects’ is sufficiently vague to encompass all the activities that aim to disrupt, deny, deceive or destroy an adversary’s IT systems. At the same time, the key reference points in the literature on cyber warfare offer several good examples of how future cyber effects are currently imagined. In the rest of this section, I suggest placing these examples into four categories, thereby laying the foundation for reflection on the opportunities and challenges associated with integrating these effects in NATO operations.

## Cyber Operations Centre

### CYOC Fails

#### CYOC ineffective – structural constraints in alliance and CYOC means only info sharing not cyber defense – deterrence posture invites attacks

Jacobsen, 2022

[Jeppe, PhD candidate Danish Institute for International Studies and the University of Southern Denmark and former coordinator of Denmark’s cyber diplomacy in European Union and NATO, "Cyber Offense in NATO: challenges and opportunities", International Affairs, Vol. 97, Issue 3, May 2021, https://academic.oup.com/ia/article-abstract/97/3/703/6205395, accessed 7/1/22, GDI-cc]

Furthermore, if the establishment of CYOC is an attempt to signal defen- sive strength and unity in cyberspace, it remains difficult to imagine that such signalling would dissuade adversaries from trying to penetrate NATO and allied systems. CYOC does not change the fact that NATO is not tasked to govern and secure national IT systems. In an operational setting, states might connect to each other through so-called federated mission networking;60 but there is no tradition of ceding control of the deployed national networks to NATO during military opera- tions. Hence, CYOC can only realistically seek to become a hub for cyber-threat information-sharing and to support states’ coordination and synchronization of various national responses to these threats. In other words, CYOC is unlikely to become an active defender in cyberspace that causes doubt in the adversary’s evaluation of its own cyber capabilities. This also means that even if CYOC’s coordination and information-sharing efforts manage to contribute to the denial of intrusions into allied systems, an adversary’s military is unlikely to be deterred from trying to hack these systems. In fact, **actively articulating that CYOC is supposed to deter (through denial) a perceived adversary such as Russia from hacking NATO and allied operational systems creates an incentive to do just that and thereby show that the alliance is incapable of doing what it says it seeks to do**. However, the renewed concern about Russia’s intentions in NATO member states since 2014 is not confined to the need to deter hostile military invasions or paramilitary activity. It also encompasses a range of subversive, non-military activities that have become available and are often considered part of a broader Russian strategy of ‘hybrid warfare’.61 Can CYOC and the integration of cyber effects deter the non-military hybrid activities that have become possible with the new information and communication technologies?

#### CYOC fails – current request based model lack coordination and flexible communication

Jacobsen, 2022

[Jeppe, PhD candidate Danish Institute for International Studies and the University of Southern Denmark and former coordinator of Denmark’s cyber diplomacy in European Union and NATO, "Cyber Offense in NATO: challenges and opportunities", International Affairs, Vol. 97, Issue 3, May 2021, https://academic.oup.com/ia/article-abstract/97/3/703/6205395, accessed 7/1/22, GDI-cc]

While these challenges are likely to persist, the cyber effects that constantly cause temporary annoyances hold a largely unappreciated potential in military opera- tions. Even though each of these effects is unlikely to have a measurable strategic effect on its own, they stay true to the dynamic cyber environment while being able to drain resources and cause confusion and doubt. To embrace this poten- tial fully, CYOC needs to adopt a more flexible and open-ended approach when requesting cyber effects. A focus on highly targeted effects requested at a specific time needs to be supplemented by more attention to requests that give member states the freedom to contribute with a variety of (offensive and actively defensive) effects when they become available. This means, for example, a willingness from NATO to accept member states’ reluctance to share cyber intelligence and to give up exclusive control over deciding on potential targets. To make SCEPVA work, there must be a constant line of communication between the national cyber units, CYOC and the NATO commanders to ensure rapid decision-making on whether to use cyber effects when they become available.

**If NATO displays this willingness and maintains this line of communication, the integration of cyber effects will become as effective as possible for an organiza- tion without close intelligence cooperation. CYOC, however,—even in its more flexible versions—is not likely to fulfil NATO’s stated ambition to strengthen its broader deterrence by integrating offensive cyber effects in its operations.**47 The next section explains why.

## Cyber signaling - nuclear

### Cyber signaling – escalation nuclear use

#### Ambiguous cyber signaling in nuclear crisis context increases risk of misperception – even if in conventional conflicts cyber signaling effective

Lonergan and Yarhi-Milo, 2022

[Erica, assistant professor in the Army Cyber Institute at West Point, and Keren, director of the Arnold A. Saltzman Institute of War and Peace Studies at Columbia University, "CYBER SIGNALING AND NUCLEAR DETERRENCE: IMPLICATIONS FOR THE UKRAINE CRISIS", War on the Rocks, 4/21/22, https://warontherocks.com/2022/04/cyber-signaling-and-nuclear-deterrence-implications-for-the-ukraine-crisis/, accessed 7/4/22, GDI-cc]

What are the implications of this for the current Ukraine crisis? Thus far, while cyber operations have been used on both sides of the conflict, they have not played a decisive role on the battlefield. So far, the United States has been focused on providing cyber defense support to Ukraine and NATO, reportedly to include dispatching Cyber Command’s cyber mission teams to Eastern Europe, as well as seeking to deter potential Russian cyber retaliation in response to U.S. and Western sanctions, especially attacks on U.S. critical infrastructure.

However, if the nuclear dimension of the crisis becomes more acute, policymakers may be tempted to turn to cyber operations to signal resolve to deter Russia in the nuclear domain. Such an approach could be seen as particularly appealing precisely because cyber operations are not kinetic and, therefore, less dangerous than other military moves. But this could have the inverse effect of making nuclear escalation, rather than deterrence, more likely, for the following reasons.

In 2020, Russia clarified its nuclear declaratory policy to state that Russia reserves the right to use nuclear weapons under a range of contingencies, including an adversary attack against “critical governmental or military sites of the Russian Federation, disruption of which would undermine nuclear forces’ response actions.” Cynthia Roberts has suggested that this particular scenario “likely include[s] cyber attacks against command and control infrastructure and/or attempted leadership decapitation.” Similarly, Dmitry Stefanovich wrote that “[t]here is a wide consensus within the Russian expert community that this also includes possible cyber threats as well as other non-nuclear dangers.” Interestingly, Russia’s declaratory policy contains parallels to the implicit link between cyber attacks and nuclear use contained in the 2018 U.S. Nuclear Posture Review. That document notes that the United States would consider using nuclear weapons under “extreme circumstances,” including “significant non-nuclear strategic attacks … [such as] attacks on U.S. or allied nuclear forces, their command and control, or warning and attack assessment capabilities.”

Therefore, a hypothetical attempt by the United States to conduct a cyber operation against Russian nuclear command, control, and communication systems for signaling purposes, such as to demonstrate resolve or convey a desire to deter the use of nuclear weapons could in practice make their use more likely. Unlike most cyber operations, which rely on secrecy, signals are meant to be seen. And to be sufficiently credible, this kind of cyber operation would have to demonstrate an ability to cause a meaningful effect against Russia’s nuclear systems, rather than a low-cost, unsophisticated cyber operation. Therefore, assuming such an attack were feasible, the chances are greater in this scenario that Russia could interpret U.S. cyber signals as an attack against its critical military systems.

The problem is that, more often than not, cyber operations are ambiguous signals. There is evidence that states can use cyber operations under some (narrow) conditions to signal a desire to de-escalate international crises. But **these findings do not extend well to nuclear crises where clarity, rather than uncertainty, is important for stability**. The use of cyber operations to defuse crises have involved cyber signaling short of war, not during an ongoing conventional conflict involving nuclear powers. And they have not involved cyber operations targeting a state’s nuclear command and control where states, like Russia, have already staked out declaratory policies. Moreover, states are still at a nascent stage in developing shared indices to inform assessments of intent in cyberspace, especially when it comes to cyber operations in nuclear crises.

Therefore, even if Russia would not take the cataclysmic step of escalating to the first use of nuclear weapons in response to a U.S. cyber operation, it could misinterpret U.S. signaling efforts and take measures to make nuclear use easier (such as making warheads operational, dispersing forces, pre-delegating authority, or increasing automaticity). **These readiness measures could increase the chances of inadvertent or even accidental escalation.**

### Cyber signaling bad – risks escalation

#### Cyber operations for deterrent purposes risks escalation

Lonergan and Yarhi-Milo, 2022

[Erica, assistant professor in the Army Cyber Institute at West Point, and Keren, director of the Arnold A. Saltzman Institute of War and Peace Studies at Columbia University, "CYBER SIGNALING AND NUCLEAR DETERRENCE: IMPLICATIONS FOR THE UKRAINE CRISIS", War on the Rocks, 4/21/22, https://warontherocks.com/2022/04/cyber-signaling-and-nuclear-deterrence-implications-for-the-ukraine-crisis/, accessed 7/4/22, GDI-cc]

So far, the Biden administration has attempted to dismiss Russia’s announcement as irresponsible saber-rattling. But as Putin continues issuing nuclear threats, policymakers are likely to feel growing pressure to respond. In particular, they may be tempted to find ways to signal to Russia to deter the use of nuclear weapons. One way this might be done is through cyber operations. In fact, some cyber experts are already calling for the United States to consider cyber attacks for signaling purposes. For example, writing in the Washington Post, Dmitri Alperovitch and Samuel Charap call on the Biden administration to consider a cyber “shock-and-awe demonstration” in response to a major Russian cyber attack against the West. They claim that such a response, which could include disrupting the Internet throughout Russia, would signal U.S. resolve and help prevent further escalation that they fear “could result in nuclear war.”

However, conducting cyber operations to signal deterrence would, paradoxically, increase risks of escalation. This risk is not just hypothetical, especially in light of Russia’s updated declaratory policy for the first use of nuclear weapons, which may include responses to cyber attacks. Russia has reinforced this message during the war in Ukraine. In early March, a hacking group affiliated with Anonymous claimed that it had shut down the control center of Russia’s space agency. While denying that the attack took place, Russia nevertheless warned that a cyber attack against its satellites would be a justification for war.

The Biden administration should clearly communicate that cyber operations for nuclear signaling are out of bounds, just as it declared restraint in other aspects of this conflict, like the deployment of American troops to Ukraine.

### Cyber signaling bad – nuclear use

#### Cyber operations implicate nuclear command and control in a limited way – but ambiguity of cyber operations risks use it or lose it mentality that increases risks of escalation to nuclear weapons use

Lonergan and Yarhi-Milo, 2022

[Erica, assistant professor in the Army Cyber Institute at West Point, and Keren, director of the Arnold A. Saltzman Institute of War and Peace Studies at Columbia University, "CYBER SIGNALING AND NUCLEAR DETERRENCE: IMPLICATIONS FOR THE UKRAINE CRISIS", War on the Rocks, 4/21/22, https://warontherocks.com/2022/04/cyber-signaling-and-nuclear-deterrence-implications-for-the-ukraine-crisis/, accessed 7/4/22, GDI-cc]

Policymakers and academics are attuned to the cyber risks to nuclear command and control. The practitioner community has largely focused on U.S. vulnerabilities and how to mitigate them. Scholars, in turn, worry about how cyber operations could have unintended escalatory consequences. But less attention has been paid to another likely scenario: the use of cyber operations for signaling purposes (operations with visible effects that aim to convey a message to another state) in a nuclear context. The ambiguity of cyber operations can sometimes be useful for signaling — but the same ambiguity can be dangerous during a nuclear crisis. The problem is that civilian leaders in particular, distinct from the military, are inclined to see cyber attacks as effective signaling tools.

Cyber operations could have nuclear implications, especially because modern nuclear command and control systems, like those in Russia and the United States, are becoming increasingly dependent on digital infrastructure. Nuclear command, control, and communications systems, which include early warning, information collection, and communications capabilities, alert decision-makers to impending nuclear strikes and also enable leaders to control decisions about nuclear use (or non-use). But their digital dependencies are creating opportunities for exploitation using cyber means. In a 2020 report, the Nuclear Threat Initiative found that “almost 9 out of 10 planned nuclear modernization programs involve at least some new digital components or upgrades.”

Vulnerabilities inherent in the digital infrastructure that undergird modern nuclear systems provide opportunities for actors to engage in cyber espionage — gaining access to a network or system to steal information — or even conduct cyber attacks. Hypothetically, a cyber power like Russia could conduct a cyber attack against a U.S. early warning satellite to degrade its functionality. This has become an urgent concern for practitioners. U.S. Strategic Command, for instance, is currently working to “operationally harden NC3 systems against cyber threats.” Congress has also gotten involved, requiring the Defense Department to evaluate the cybersecurity of major weapon systems. And the Government Accountability Office has published multiple reports decrying the state of cybersecurity and scope of vulnerabilities of weapon systems, including elements of the nuclear triad.

From an academic perspective, scholars have investigated how cyber operations targeting nuclear systems could exacerbate escalation risks. Focusing on nuclear forces, early research, such as work by Martin Libicki, was skeptical of the dangers posed by cyber operations. Nuclear forces were seen as being largely immune from digital attacks because they were “air gapped,” meaning that they were separated from information technology systems.

However, as nuclear systems have become increasingly intertwined with the digital environment — not to mention the dual-use nature of many elements of nuclear command, control, and communications systems (like early warning or position, navigation, and timing satellites) — the protection offered by being segregated from the internet is less robust. Jacquelyn Schneider, Benjamin Schechter, and Rachael Schaffer, for instance, ran a series of wargames demonstrating that decision-makers in hypothetical crises are likely to use their cyber exploits against an adversary’s nuclear systems. They found that this could have negative effects on states’ respective nuclear strategies, especially decisions to pre-delegate nuclear launch authority or automate nuclear responses. Erik Gartzke and Jon Lindsay argue that the clandestine nature of cyber operations means that one state could secretly gain access to an adversary’s nuclear command, control, and communications systems, giving the former an information advantage or even creating an incentive for the latter to use its nuclear weapons out of the fear that it may lose them. James Acton notes that the difficulties of distinguishing between cyber espionage and attack could lead a state to misperceive the intent behind a cyber operation, generating a similar “use it or lose it” calculus.

### Cyber signaling – misuse increases risk

#### Cyber signaling ineffective because of difficulties – but use by civilian leadership increases risk of escalation that outweigh benefits

Lonergan and Yarhi-Milo, 2022

[Erica, assistant professor in the Army Cyber Institute at West Point, and Keren, director of the Arnold A. Saltzman Institute of War and Peace Studies at Columbia University, "CYBER SIGNALING AND NUCLEAR DETERRENCE: IMPLICATIONS FOR THE UKRAINE CRISIS", War on the Rocks, 4/21/22, https://warontherocks.com/2022/04/cyber-signaling-and-nuclear-deterrence-implications-for-the-ukraine-crisis/, accessed 7/4/22, GDI-cc]

But all of this focus on cyber operations causing nuclear escalation may be misplaced and, more importantly, distract policymakers from the dangers of a more plausible scenario: the use of ambiguous cyber signals during nuclear crises. Specifically, the nature of cyber operations reduces their inherent escalatory potential, particularly when compared to other ways a state could attack an adversary’s nuclear forces or command, control, and communications systems, like a direct counterforce strike or employing anti-satellite weapons. But their misuse as a signaling tool could do more harm than good.

First, successfully conducting cyber operations against strategic targets, like nuclear systems, is harder than the conventional wisdom might suggest. It requires a means of gaining access to a particular system and developing an exploit to cause a desired effect — and then maintaining persistent (and stealthy) access to be able to conduct an offensive operation at the desired time. Moreover, the overall outcome may be unpredictable and net less-than-desirable results.

Second, even if a state is able to conduct these kinds of operations, they typically prefer to do so in secret — and this mitigates some escalation concerns. That’s because, to cause an escalatory response, a state like Russia would have to uncover a cyber operation during a particular time period — such as while the Ukraine conflict is unfolding. For example, Russia would have to detect a cyber operation against a nuclear command and control system to cause Putin to perceive a “window of vulnerability,” perhaps assessing that it is part of a U.S. or NATO counterforce strategy to disable Russia’s ability to retaliate with nuclear weapons. But the likelihood of these circumstances arising is low because — unless a state is trying to signal with a cyber capability — it will try to keep these kinds of sensitive operations secret. Therefore, the chances of such an operation being discovered at a particular time period are relatively small.

Finally, even if, hypothetically, Russia was to discover a cyber operation taking place, the likelihood of it leading to escalation is low. This is due to the virtual nature of cyber “weapons” — they rarely cause destruction in the physical world, let alone permanent damage. For example, even Russia’s 2015 cyber attack against Ukraine’s power grid, an important example of a strategic cyber attack against civilian critical infrastructure, only resulted in service disruptions for a few hours. During the current conflict, Russia-linked actors have so far been stymied in using cyber operations for strategic impact, such as the failed cyber attack by the group Sandworm against Ukraine’s power grid.

Taken together, this reasoning suggests that, in practice, cyber operations may not rise to a level that would cause a state like Russia to actually fear the integrity of its nuclear command, control, and communications systems, creating few reasons to escalate to the level of nuclear employment.

Civil-Military Relations and the Risks of Cyber Signaling in Nuclear Crises

Differences in how civilian and military leaders see the use of military power are likely to be even more salient in cyberspace, for three reasons. First, cyberspace is a highly technical environment where civilians typically lack subject matter expertise. Practitioners are likely to have far more up-to-date operational experience and, therefore, fluency with the technical issues and constraints posed by cyber operations than civilian leaders (even those with prior and, potentially, outmoded experience). Cyberspace is also a [highly classified](https://mwi.usma.edu/overclassification-and-its-impact-on-cyber-conflict-and-democracy/) environment — one in which information is highly segmented and only accessible to a select group of individuals. Therefore, some civilian officials may not be privy to all of the details surrounding cyber operations. Finally, unlike other technical and secretive environments, cyberspace has an additional element that makes it even more difficult for non-experts to grasp its nature. Specifically, cyberspace is also an esoteric environment; cyber operations and their effects are not easily visible in a way that other types of military capabilities are, making it difficult to conceptualize their utility in a tangible manner.

There is evidence supporting this idea. For instance, senior civilian leaders across multiple U.S. administrations, as well as in Congress, typically describe cyber operations as useful for signaling deterrence and resolve. Chris Inglis, the Biden administration’s inaugural National Cyber Director, [described](https://www.afcea.org/content/national-cyber-leader-ponders-response-vectors-cyber-adversaries) how he’d “like to change the decision calculus of those who transgress in this space,” and contemplated that “[p]erhaps our actions should be felt by an adversary. They should know that they have just felt the hand of whomever.” Similarly, Senator Angus King, [discussing](https://www.washingtonpost.com/politics/2021/06/30/cybersecurity-202-angus-king-says-its-time-get-tougher-russian-hackers/) the threat of Russian-linked ransomware attacks in the summer of 2021, noted that he wants “somebody … in the Politburo to say, ‘Gee, boss, I’m not sure we ought to do this because we’re liable to get whacked in some way by those Americans.’”

John Bolton, former national security advisor, in multiple public statements, has depicted the purpose of U.S. cyber operations — especially offensive ones — as a means of influencing adversary perception. He [described](https://news.grabien.com/making-transcript-white-house-press-briefing-national-cyber-strateg) how the employment of offensive cyber power creates “structures of deterrence, so that it’s publicly known,” and that “it is important that our adversaries know [that] …we have authorized offensive cyber operations to … demonstrate to our adversaries that the costs of engaging in operations against us is higher than they want to bear.” Michael Daniel, the Obama administration’s cyber czar, [depict](https://www.yahoo.com/news/obama-cyber-chief-confirms-stand-order-russian-cyberattacks-summer-2016-204935758.html?guccounter=1)ed the purpose of imposing costs on Russia in response to its 2016 election interference as “to openly demonstrate that we could do it as a deterrent and also clandestinely disrupt their operations as well.”

In contrast, while some military leaders do talk about cyber deterrence, the language they employ is anchored in tactical and operational objectives, rather than aiming to influence adversary perception and decision-making. This is evident in how both civilian and military leaders use the language of “imposing costs.” Military leaders tend to describe cost-imposition as supporting the disruption, degradation, denial, or destruction of adversary offensive capabilities and operations. For instance, in December 2021, Gen. Paul Nakasone, commander of U.S. Cyber Command and director of the National Security Agency (NSA), described “imposing costs” against Russian-linked ransomware groups as the goal in itself. The month prior, at the November 2021 Aspen Security Forum, he argued for the United States to impose costs in cyberspace, but stated that a traditional deterrence strategy “does not comport to cyberspace.” In another example, in 2019, Lt. Gen. Stephen Fogarty, commander of Army Cyber Command, voiced skepticism about cyber deterrence in remarks about defending the 2020 elections against cyber interference, noting that “I don’t know of a single thing we could do that would prevent [adversaries] from competing, but I want to impose as much cost on them as possible.”

## Military to military exercises – general

### Military to military exercises – general

#### Military to military cyber exercises like Locked Shield fail – multiple warrants

**Achberger and Smeets, 2022**

[Brita, Research Assistant specializing in international cybersecurity politics, and Max, Senior Researcher at the Center for Security Studies (CSS) at ETH Zurich and Director of the European Cyber Conflict Research Initiative, "The Opportunities and Challenges of Military Cyber Exercises", Council on Foreign Relations, 3/24/22, https://www.cfr.org/blog/opportunities-and-challenges-military-cyber-exercises, accessed 6/30/22, GDI- CC]

It is May 2019 and a conference room of the Nordic Hotel in Tallinn is once again transformed into a situation room. There is a large scoreboard and map on the wall, and several tables, each with multiple screens set up. The conference room is filled with people wearing different color shirts and lanyards that indicate their team and role. A government delegation is being given a tour from an exercise organizer wearing green. This is the scene of the largest international technical cyber exercise in the world, Locked Shields, run by the North Atlantic Treaty Organization (NATO) Cooperative Cyber Defence Center of Excellence (CCDCOE)

CCDCOE started organizing Locked Shields in 2012–preceded by the Baltic Cyber Shield, a one-off exercise in 2010. In 2021, Locked Shields had over two thousand participants. Thirty countries have participated so far, including a NATO alliance team and non-NATO member states Australia and Japan. Over the past decade, military exercises have increasingly focused on cyber-related scenarios, which present unique opportunities and challenges for military planners. The main opportunities of military cyber exercises lie in the collection and analysis of data and the signaling of operational capability. The challenges to military cyber exercises stem from difficulties defining an appropriate ruleset and the resources required to create a realistic training environment with realistic timeframes and dynamics.

Military cyber exercises come in various shapes and forms: from specific, nationally oriented exercises such as Operation Eligible Receiver, organized by the U.S. Department of Defense in 1997, to more general, internationally oriented exercises like Cyber Coalition, organized annually by NATO. Some exercises are more offense-oriented, such as Crossed Swords, while other games lay the emphasis on defense, like Locked Shields.

Military cyber exercises are generally run in a virtual environment. The benefit of which is the organizer’s ability to collect data as the activities of different teams can be more easily recorded. Whilst traffic logs and other data are not always easy to digest, it often creates the opportunity for more granular analyses of moves ex post facto.

Signaling cyber capability is notoriously difficult. However, military cyber exercises can be used as a means of signaling capability and willingness to conduct or respond to cyber operations. “You cannot parade computer code on the streets of Moscow”, but you can create a scenario in which you successfully mitigate simulated malicious code in Moscow’s transportation infrastructure.

But military cyber exercises also come with their own challenges. It is difficult to create a realistic exercise without a realistic battleground. Setting up an environment for military cyber exercises is not cheap; an extreme case is the U.S. Department of Defense’s plans for a new global cyber training environment, which is expected to cost roughly $1 billion.

Second, military cyber exercises hardly ever stretch longer than a few days. This may set misleading expectations about the nature of cyber operations. We know that unique decision-making dynamics in cyber operations stem from their timeframe. Preparation of more advanced cyber operations takes time, a reality which may have affected the ability of Russian hackers to attack Ukrainian systems. Also, it often takes considerable time to move from initial access to fulfilling strategic objectives in a cyber operation. The installation of a backdoor in one phase may lead to the dropping of malware only many months later.

The short duration of military cyber exercises can also negatively impact officials’ conception of the strategic potential of this space. Military cyber exercises generally revolve around a set of highly disruptive or destructive cyberattacks for a relatively short period–a typical scenario is an attack on critical infrastructure by an adversarial state. However, much of what we have been observing in cyberspace are multi-year campaigns comprised of linked cyber operations, with the objective of achieving strategic outcomes without the need of armed attack. Incorporating this understanding of the multifaceted and simultaneous nature of cyber activity is challenging under such time restrictions.

Also, in the case of Locked Shields, it is hard to promote NATO’s principles of collective defense. Inter-team cooperation and collaboration between the countries’ blue teams in tackling cyber incidents has been a goal since Locked Shields’ beginnings. In early versions of the exercise, teams could score extra points for cooperation with other teams. However, it proved difficult to measure cooperation in a meaningful way during Locked Shields and reconcile it with the competition element of the exercise.

Finally, one inevitable aspect of military exercises is that they come to an end. And while it is hard to predict the cyber future, one thing we can be certain about is that cyber operations are not ending any time soon. At the conclusion of the three days, Locked Shields crowns a winning defending blue team based on their performance under attack and a score they receive. Victory in cyberspace will never be this clear.

## Memo of Understanding

#### MOU won’t work to solve issues with the allies’ coordination on offensive cyber operations

**Smeets,** ETH Zurich, Center for Security Studies, **2020**

[Max “U.S. Cyber Strategy of Persistent Engagement & Defend Forward: Implications for the Alliance and Intelligence Collection” Intelligence and National Security vol 35, 2020 – Issue 3, Taylor and Francis Online accessed 7/5/2022 GDI-TM]

Conclusion and Discussion

The purpose of this paper was to provide a benefit-risk assessment of US strategy for its allies and intelligence collection. Whilst the U.S. government’s mission to persistently engage with adversaries may have benefits for allied states, the paper identified several avenues how the strategy leads to negative implications for the alliance. To conclude, it is therefore worth considering how these risks can be mitigated.

First, the principles of persistent engagement and defend forward are often jointly discussed. How the two principles relate to each other, however, remains unclear. According to some, persistent engagement is an ‘operationalization’ of the defend forward concept. Others believe there is a difference between the two concepts. If the latter is the case, it is important to assess to what degree a strategy of persistent engagement necessitates ‘defending forward’ and contesting adversaries wherever they are. In other words, the question is whether sufficient friction can be created without causing disruption in allied networks. Second, terminology about terrain in cyberspace is frequently confused by policymakers and experts. The U.S. government needs to (re)assess how its terminology of terrain in the physical domains applies to cyberspace.

Last, NATO allies should consider establishing memoranda of understanding on offensive cyber effects operations in systems or networks based in allied territory.xlvii The goal of the proposed memorandum would be to reduce discord among the allies; enhance trust, transparency and confidence between allies; and improve the effectiveness of disrupting and deterring adversaries’ operations in cyberspace. The scope of the memorandum would include: i) developing a common notification equity framework for out-of-networks operations which seek to achieve cyber effects in allied systems or networks; ii) identifying procedures for communicating the consideration and conduct of offensive cyber effects operations between states against systems or networks in allied territory; and iii) identifying technical solutions and administrative documentation required for the continuous exchange of information on offensive cyber operations. In writing the memorandum, states first and foremost should agree on the equities involved in permitting signatories to conduct cyber effect operations in each other’s networks—and the relative weight of those equities. Equities that should be considered include: i) the ability of an actor to take action to negate known threats on or to the other parties’ networks and systems; ii) the likelihood that an action will negate known threats; iii) the imminence and scale of the threat; iv) the risk of collateral damage; v) whether the computer system or network is government-owned or privately owned; and vi) the certainty that the system or network will be used to achieve strategic effects by the adversary.xlviii Finally, though the memorandum of understanding may help in promoting stability and enhancing confidence amongst allies, it is not a silver bullet. It can only reduce allied concerns rather than mitigate them. Military cyber organizations may still conduct effect-based operations in allied territory without consent, leading allies to assert that their sovereignty has been violated. Furthermore, there is another crucial player involved. As Gen. Nakasone noted in the Joint Force Quarterly article, cyberspace is owned largely by the private sector. They deserve a seat at the table as well.xlix

## Offensive cyber BAD/not so good

### \*\*notes\*\*

Note that some of these cards are descriptive of the incentives bc of SCEPVA – if the plan alters that structure then some won’t apply

The other OCOs bad card or would fail cards are both descriptive of the SQuo and probably the GDI aff bc no evidence that the military to military exercises could overcome coordination issues

### Squo fails – no coordination

#### SQuo NATO offensive cyber capability policies deviate from normal coordination approach - fail to account for growing number of states with capability

**Jensen, Institute for Strategy and War Studies, 2022**

[Mikkel Storm, “Five good reasons for NATO’s pragmatic approach to offensive cyberspace operations”, Defense Studies, 30 May 2022, Francis and Taylor Online, 6/29/22, <https://doi.org/10.1080/14702436.2022.2080661>, GDI – LL]

Introduction

For decades, few NATO members, predominantly the US, could conduct offensive cyberspace operations (OCO). Hence, there was little requirement for coordination with allies. This has changed: the economical threshold to acquire offensive cyberspace operations capabilities (OCOC) has fallen to a level where more than half of NATO’s members now claim to have these means. These developments have made NATO adjust.

Historically, NATO’s planning and coordination has been based on shared knowledge of the members’ military capabilities, to a degree even their nuclear capabilities. In the cyber domain, the principle has evolved to include the allies’ emerging defensive cyber capabilities. NATO’s approach to OCOC, however, deviates radically: NATO’s doctrine merely integrate offensive cyber effects, that is, allow members to offer them in operations without sharing information with allies on what OCOC are available or how the effects are delivered. NATO is a well-established mechanism to coordinate the members’ military means. This core function is the bedrock of military strategy for some small members, for example, Denmark. Hence, NATO’s and the individual members’ notable divergence from historical practice when it comes to OCOCs presents a puzzle.

The technical and tactical characteristics particular to OCOCs differ significantly from conventional military means. Among the particular characteristics are the extraordinarily strong incentives to keep any aspect of OCOCs secret, even from other allies. This creates new and unique dilemmas for allies and inhibit OCOCs’ use in military alliances. Either the allies providing OCO’s effects risk sharing sensitive information on the OCOCs or the allies, who depend on the provided effects, must accept the proposed effects without sufficient knowledge of the deployed OCOCs to assess their efficacy, legality, or impact on own offensive or defensive cyberspace operations.

The constraints on NATO’s ability to coordinate OCOCs will likely remain insur- mountable for years to come. This may explain why NATO developed the Sovereign Cyber Effects, Provided Voluntarily by Allies (SCEPVA) concept which allows the allies to circumvent some of the challenges associated with coordination (NATO 2020, 5,16). The SCEPVA-construct enable integration of OCOCs in operations while sharing little or no information on the deployed means. SCEPVA’s are in NATO’s own words not the most effective way to fully utilize the allies’ combined OCO potential (NATO 2020, 26). However, the construct provides a pragmatic doctrinal framework for NATO to train and develop procedures and eventually integrate the effects of OCO in operations.

#### Allies can’t solve – their institutional capacity to limited

**Smeets,** ETH Zurich, Center for Security Studies, **2020**

[Max “U.S. Cyber Strategy of Persistent Engagement & Defend Forward: Implications for the Alliance and Intelligence Collection” Intelligence and National Security vol 35, 2020 – Issue 3, Taylor and Francis Online accessed 7/5/2022 GDI-TM]

Last year the NATO alliance reached a landmark that went largely unnoticed: there are now more NATO member states that have publicly declared they are seeking to establish an institutional capacity within the military forces to conduct cyber effects operations than there are member states that have remained publicly silent on this issue.xliv Yet, most NATO members are still at the early stages of organizational development - and pour relatively few resources into their military cyber organizations to conduct cyber effects operations.xlv Their operational capacity is limited. France and Germany stand out for the extent of resources officially allocated to their military cyber organizations (beyond the Five-Eyes) - but public statements about these figures are generally hard to interpret and compare given distinct institutional design across military cyber organizations of states.xlvi This risk is therefore less significant for the short term, but is likely to grow in the medium to long term.

### SQuo – NATO lacks offensive coordination

#### NATO lacks effective coordination of offensive cyber capabilities outside of warfighting context, results in failure to deter most significant threats to NATO in cyber grey zone

**Lonergan** , assistant professor in the Army Cyber Institute at West Point and research scholar at the Saltzman Institute of War and Peace Studies at Columbia University **and Montgomery**, senior director of the Center on Cyber and Technology Innovation at the Foundation for Defense of Democracies, **2022**

[Erica D. and Mark “PRESSING QUESTIONS: OFFENSIVE CYBER OPERATIONS AND NATO STRATEGY” Modern War Institute, 01.25.22 <https://mwi.usma.edu/pressing-questions-offensive-cyber-operations-and-nato-strategy/> accessed july 5 2022 GDI-TM]

NATO members are in the midst of a crisis. With Russia massing troops along its border with Ukraine and moving additional forces to Belarus ostensibly to conduct joint military exercises, policymakers fear that Russia is on the precipice of invading Ukraine and taking additional territory by force—similar to Russia’s annexation of Crimea in 2014. But, even if Russian President Vladimir Putin ultimately chooses not to launch a direct, conventional invasion of Ukraine, it is highly likely that he will continue to pursue Russian strategic objectives in the gray zone short of war. The crisis over Ukraine underscores the challenges NATO faces in competing with Russia in the gray zone—especially in cyberspace.

Russia has no such limitations in the gray zone. In addition to traditional forms of irregular warfare, such as the use of plausibly deniable proxy forces (Putin’s “little green men”), Russia has long relied on cyber operations to subvert and undermine rival governments while avoiding actions that would cross a threshold prompting an overwhelming retaliation. Indeed, in tandem with Russia’s conventional military buildup, Ukrainian government agencies were struck with a spate of website defacements. Microsoft also revealed that it had discovered destructive malware in some Ukrainian government systems, which Ukrainian officials have linked to the Belarusian group GhostWriter. Belarus has close ties to Russia, and observers have speculated that Belarus may have been operating in cyberspace on Russia’s behalf.

While Ukraine is not a NATO member, the current situation underscores the enduring strategic challenge the alliance faces in addressing the cyber threat posed by Russia and other actors. In particular, because cost imposition is an integral part of any deterrence strategy (and has been part of NATO’s conventional deterrence strategy), the alliance has begun to explore how it could incorporate offensive cyber operations as a component of its cyber deterrence posture. But, while NATO took important steps to address cyber defense, it took nearly a decade after Russia’s 2007 cyberattack against Estonia to begin to seriously address the issue of offensive cyber operations. Moreover, NATO cyber policy has traditionally focused on cyber operations in a warfighting context—a focus that comes at the expense of considering cyber operations below the level of warfare. As the recent cyberattacks against Ukraine illustrate, the gray zone just beneath the threshold of armed conflict is where NATO faces its most significant cyber threats. With NATO in the middle of conducting a comprehensive initiative, NATO 2030, to strengthen the alliance, it should incorporate an assessment of the role of cyber operations in routine competition.

#### Squo recognition of need for offensive cyber too limited and fails respond to the cyber threat environment NATO faces outside of active warfighting

**Lonergan** , assistant professor in the Army Cyber Institute at West Point and research scholar at the Saltzman Institute of War and Peace Studies at Columbia University **and Montgomery**, senior director of the Center on Cyber and Technology Innovation at the Foundation for Defense of Democracies, **2022**

Offensive Cyber Operations in NATO Strategy Above and Below the Level of Warfare

Historically, NATO’s cyber posture has largely focused on defense and resilience—and this continues to form the bulk of NATO’s approach. The alliance maintains that its “main focus in cyber defence is to protect its own networks (including operations and missions) and enhance resilience.” At the 2014 Wales summit, NATO endorsed the Enhanced Cyber Defence Policy, which affirmed that cyber defense is part of collective defense and that the alliance would incorporate cyber defense into its planning and operations. In 2016, NATO members pledged to improve their cyber defenses through training, education, exercises, and information sharing.

But the seeds were also planted in 2016 for NATO to consider a potential role for offensive cyber operations. That year, the alliance recognized cyberspace as a domain of military operations, comparable to land, sea, and air. At the 2018 Brussels summit, NATO began to more seriously consider offensive cyber operations. Specifically, NATO created the Cyberspace Operations Centre to coordinate requests for member states to provide offensive cyber effects through the Sovereign Cyber Effects Provided Voluntarily by Allies process. Following the 2018 summit, then-Secretary of Defense James Mattis stated in a press conference that five states—the United States, the United Kingdom, Denmark, the Netherlands, and Estonia—were contributing cyber forces to “help NATO fight in this important domain.” More recently, in June 2021, NATO convened in Brussels and committed to a Comprehensive Cyber Defence Policy. A key feature of the new policy is the prominent role of offensive cyber operations. In Brussels, member states committed to “employ the full range of capabilities at all times to actively deter, defend against, and counter the full spectrum of cyber threats.”

NATO’s shift to incorporating offensive cyber operations into existing strategy and policy has focused on integrating offensive effects into conventional military plans and operations in the context of a conflict. While NATO’s updated strategy is a positive development, its limited focus on conflict scenarios for employing cyber power fails to accurately account for the cyber threat environment NATO faces—particularly the mismatch between the alliance’s clear distinction between wartime and peacetime and the approach of adversaries like Russia, who adopt a competition-conflict continuum. Additionally, the focus on employing offensive cyber during a high-end conventional fight is also not consistent with how several NATO members are already engaged in gray zone offensive cyber operations.

### No solvency – offensive integration

#### Squo solves – NATO Cyber Rapid Reaction forces already integrating into defense – no consensus on expansion to offensive capabilities

**Iftimie,** Eisenhower PhD Candidate Fellow, NATO Defense College, and Senior Advisor, European Union Research Center, George Washington University School of Business**, 2020**

[Ion, “NATO’s needed offensive cyber capabilities” NDC POLICY BRIEF No. 10 – May 2020 <https://www.ndc.nato.int/news/news.php?icode=1441#:~:text=This%20Policy%20Brief%20looks%20at,cyber%20capabilities%20into%20its%20operations> accessed 7/5/22 GDI-TM]

NATO Cyber Rapid Reaction teams are already equipped to conduct defensive cyber operations in support of member states if called upon. A mandate of cyber defence and security implies, however, that NATO also starts to engage in active military measures to deny, degrade, disrupt, deceive, or destroy an adversary’s offensive cyber capabilities. This requires the development of not only offensive cyber A2/AD capabilities by Allies, but also the restructuring of the NATO command structures, policies, processes (procurement, intelligence, operations, etc.) and engagements needed to integrate them by the Alliance. NATO coordination with both national and regional entities charged with cyber security aspects will, in particular, need to be enhanced. Many agreements already exist in the realm of defensive cyber at national and regional levels (as seen with the 2016 NATO-EU Technical Arrangement on Cyber Defence), but political consensus among Allies is missing on whether they should be expanded to incorporate the collective use of offensive cyber A2/AD capabilities.

### OCOCs coordination fail – national incentives

#### Member states incentivized to keep their best cyber effects – won’t be able to coordinate use

**Jensen, Institute for Strategy and War Studies, 2022**

[Mikkel Storm, “Five good reasons for NATO’s pragmatic approach to offensive cyberspace operations”, Defense Studies, 30 May 2022, Francis and Taylor Online, 6/29/22, <https://doi.org/10.1080/14702436.2022.2080661>, GDI – LL]

\*OCO - offensive cyberspace operations

\*OCOC - offensive cyberspace operations capabilities

This article fills a gap in the strategic literature by investigating some effects of OCOCs and OCO’s on alliances. NATO is a relevant empirical case study: it is by far the world’s largest collective defense arrangement and at least 16 members already claim to have or strive to get OCOCs. At least nine of these have pledged to make them available in support of NATO operations (Vavra 2019). Furthermore, NATO provide some empirical evidence to the analysis, having worked with the challenges of integrating member states’ emerging offensive cyber capabilities since at least 2016 when the alliance acknowledged cyberspace as an operational domain (Ablon et al. 2019, 1). This has produced both academic debate and concrete outcomes, that is, organizational adaptations and doctrine like the Cyberspace Operations Center (CyOC) and the AJP-3.20, Allied Joint Doctrine for Cyberspace Operations (Brent 2019; NATO 2020).

After this introduction follows a presentation of definitions, methodology and a short review of current strategic literature on this topic. Then, the article describes NATO’s current approach to the allies’ OCOCs and including OCO’s effects in operations and compares with NATO’s approaches to conventional weapons, nuclear weapons, and defensive cyber means to identify differences. The initial conclusion is that NATO’s approach to coordination of allies’ OCOCs is indeed different and much more restricted than to the other three categories.

The second part of the article present the main argument: five technical and tactical characteristics of OCOCs cause special dilemmas that make their coordinated use in alliances more difficult than conventional military means. Based on the identified chal- lenges to coordination of OCOCs, the article concludes that NATO’s ambition will likely remain limited to their inclusion rather than coordination. The article suggests that this situation may change if the nations providing OCO effects differentiate more between “mundane” OCOCs based on standard tools that are sharable, and advanced, tailored OCOCs based on sensitive information that will likely remain outside the scope of full coordination between allies. Also, a sufficiently significant crisis and the need to respond will likely induce NATO members to overcome some of the concerns that inhibits coordination between allies, especially if information exchange can be limited to a minimum of member states.

#### OCO incentive structures the same in alliances – no matter how small and cohesive

**Jensen, Institute for Strategy and War Studies, 2022**

[Mikkel Storm, “Five good reasons for NATO’s pragmatic approach to offensive cyberspace operations”, Defense Studies, 30 May 2022, Francis and Taylor Online, 6/29/22, <https://doi.org/10.1080/14702436.2022.2080661>, GDI – LL]

\*OCO - offensive cyberspace operations

\*OCOC - offensive cyberspace operations capabilities

The limited literature on offensive cyber, alliances, and strategy

Most academic literature on offensive cyber strategy is written from a great power perspective and does not consider its use in alliances. Instead, the literature focuses on the first-order effects of a state’s actions against its opponents. For a small state, the second-order effect on its allies of its military actions may be far more important than the first-order effect on its opponent (Jakobsen et al. 2016, 10–12).

Smeets (Smeets 2018b) and Fasana (Fasana 2018) discuss the values and risks of integration of OCOs in military operations, but do not analyze their use in coalitions. Hughes and Colarik (Hughes and Colarik 2016) encompass both small states, alli- ances and OCOCs by identifying the theoretical advantages and risks, which they expect New Zealand would incur by developing OCOCs and investigating how these could be deployed within New Zealand’s military cooperation with, for example, Australia or the U.S. Hughes and Colarik assume that New Zealand can coordinate use of OCOs in a military coalition with the U.S. or the other Five-Eyes intelligence sharing community, Australia, Canada, and United Kingdom, on a par with conven- tional means (Hughes and Colarik 2016, 173; Tossini 2017). New Zealand is not currently in any military alliance but retains very close relations with the U.S. (State Department 2020).

In a theoretical coalition involving the U.S., New +Zealand, and other Five-Eyes- members, coordination of OCOs would likely be less challenging than between NATO’s 30 members due to fewer members and the well-established Five-Eyes framework for sharing classified information. Still, this article challenges Hughes and Colarik’s assump- tion of information sharing-based coordination of OCOs between close allies by demon- strating why this is likely to involve difficult dilemmas in any alliance regardless how small and close-knit it might be.

### OCOCs coordination fail – advanced

#### The more advanced the OCO, the less likely member states sharing occurs

**Jensen, Institute for Strategy and War Studies, 2022**

[Mikkel Storm, “Five good reasons for NATO’s pragmatic approach to offensive cyberspace operations”, Defense Studies, 30 May 2022, Francis and Taylor Online, 6/29/22, <https://doi.org/10.1080/14702436.2022.2080661>, GDI – LL]

\*OCO - offensive cyberspace operations

\*OCOC - offensive cyberspace operations capabilities

Offensive cyberspace operations, capabilities, and strategy

NATO defines cyberspace as “The global domain consisting of all interconnected com- munication, information technology, and other electronic systems, networks and their data, including those which are separated or independent, which process, store or transmit data.” OCO are defined as “Actions in or through cyberspace that project power to create effects, which achieve military objectives” (NATO 2020, 4). To facilitate the present analysis, the non-doctrinal term “Offensive Cyberspace Operation Capabilities” (OCOC) is introduced to cover the capabilities, or example, technology, trained personnel, command and control, etc., necessary to enable states to conduct military OCO.

**NATO’s definitions of OCO follow the definitions of current US doctrines** – but it’s very broad. To focus the analysis, this article harks back to older US doctrines that distinguish between two different categories of OCO as shown in figure 1 below: Computer Network Attacks (CNA) and Computer Network Exploitation (CNE). While no longer officially in use, CNE and CNA are analytically very helpful categories (NIST n.d.). CNA are OCOs to disrupt, deny, degrade, or destroy information resident in computers and computer networks, or the computers and networks themselves (Joint Chiefs of Staff 1998, GL-5). The older US doctrine’s definitions of CNA effects vary slightly from, but are all covered by, the effects listed in the NATO doctrine (NATO 2020, 18). CNA’s effects are not limited to data and the associated IT-hardware, but may be inflicted on any physical hardware connected to the cyber-affected systems directly or indirectly as second or higher order effect. In the Russian 2015 “Black Energy”-attack that resulted in power outages for nearly 225,000 people in Western Ukraine, CNAs directly targeted substations’ hardware on the Ukrainian electricity distribution grid (Colatin 2021). The dramatic impact of the 2021 CNA on Colonial Pipeline, where criminals hijacked a US fuel distribution com- pany’s data, may have been second-order effects resulting from to the company’s attempts to limit the impact of the initial attack. Regardless, the CNA halted operations for days, caused a 45% drop in fuel distribution and made 17 states on the US east coast declare a state of emergency (Turton and Mehrota 2021; Panettieri 2021).

This analysis distinguishes between advanced and un-advanced OCOCs. In this regard, “advanced” does not refer to the technical complexity of the code employed, but to the degree that the offensive cyber capability is tailored to a specific target and/or dependent on comprehensive intelligence collection for its design. It is a distinction between “a small number of weapons or targeted actions and a very large number of more indiscriminate tools“ (Taillat 2019, 372). Advanced OCOCs are based on intelli- gence collected clandestinely which means sharing information on the OCOCs may jeopardize intelligence assets, means, and methods. Thus, un-advanced OCOCs are relatively common and mundane means for OCO, perhaps similar to, or copies of, means used by cyber criminals.

CNE is qualitatively distinctly different from CNA: CNE is cyber-enabled espionage, “enabling operations and intelligence collection capabilities conducted through the use of computer networks to gather data from target or adversary information systems or networks” (Department of the Army 2003, 2–11). that is, CNE is an OCO that conducts “seeing without touching” whereas CNA is an OCO intended to inflict some degree of damage.

This analysis does not include CNE or other cyber-enabled offensive operations, for example, misinformation distributed on social media and targeted by algorithms. Why? Because like CNA, CNE and cyber enabled or enhanced propaganda and misinformation can have significant strategic offensive effects (Lin 2019; Rogin 2012). However, neither CNE nor misinformation represent new qualitatively new means for states to wield coercive power. Thus, their effects on alliances, including NATO, are not new either. Admittedly, cyber brings new nuances, for example, by increasing the potential speed, scope, and scale of such operations by orders of magnitude compared to the analog past (Søilen 2016). Furthermore, CNE is arguably relevant to the present analysis due to the potential strategic side effects of alliance members’ individual tactical CNE: because CNE often is a necessary precursor to CNA, the line between CNE and CNA is blurred (Smeets 2018b, 9). Thus, it can be difficult from a victim’s perspective to assess whether CNE is “just” cyber espionage or preparations for CNA. In addition, attribution may be uncer- tain, and misinterpretations could lead an opponent to undertake unintended escalatory actions, perhaps against the entire alliance. Hence, from a theoretical perspective, ideally even CNE should be a coordinated effort in alliances. Even so, CNE is excluded from the analysis because intelligence collection always has been a prerogative of the individual NATO members and is highly likely to remain so.

Strategy is interpreted according to Yarger et al: “Strategy is all about how (way or concept) leadership will use the power (means or resources) available to the state to exercise control over sets of circumstances and geographic locations to achieve objec- tives (ends) that support state interests.” (Yarger and Boone Bartholomees 2012, 45). In this analysis, OCOCs are means that statesin this case, NATO-members, use for raisons d’état. The analysis is based on the assumption that NATO’s members are rational, self- interested states, an assumption that is admittedly over-simplifying. For example, different types of OCOCs should in principle present different levels of challenges to coordinate, as the difficulties arise from the states’ inclination to keep these means secret. This inclination should increase along with the risk they pose to, for example, sensitive intelligence assets – and fall if this risk was low. Hence, in theory, obstacles to CNA coordination should vary from trivial to insurmountable if NATO members were pragmatic about their use and classified OCOCs according to risk. However, the very limited empirical evidence suggests that most OCOCs are highly classified and “national eyes only,” leaving them in or around the insurmountable category. Still, the assumption of rational self-interested states will provide a baseline of insights in the alliance-related dilemmas emerging along with the NATO members’ increasing OCOCs.

On that note, and emphasized throughout the article, the entire topic of military OCOCs is shrouded in secrecy. This limits the analysis to available information from reputable public sources, combined with generally accepted characteristics of OCOCs as presented in the scholarly literature. To keep the analysis relevant and to stay away from hyperbolic conclusions, I am grateful to have had the opportunity to calibrate my findings through discussions with actual operators in the realm, not least former US Vice Chairman of the Joint Chiefs of Staff, General James S. Cartwright.

### OCOCs coordination fail – lack of information

#### No coordination – lack of knowledge of national effects and capabilities limit standardization of development or acquisition

**Jensen, Institute for Strategy and War Studies, 2022**

[Mikkel Storm, “Five good reasons for NATO’s pragmatic approach to offensive cyberspace operations”, Defense Studies, 30 May 2022, Francis and Taylor Online, 6/29/22, <https://doi.org/10.1080/14702436.2022.2080661>, GDI – LL]

\*OCO - offensive cyberspace operations

\*OCOC - offensive cyberspace operations capabilities

Military nuclear capabilities

Due to their enormous destructiveness, nuclear weapons are on many levels a special category. As such, NATO treats them differently. Nuclear weapons and the decision process regarding their use are strictly national for the three nuclear wielding NATO- members, the US, UK, and France.

Nevertheless, general information on nuclear capabilities are relatively accessible even from unclassified sources (Kristensen and Korda 2019b, 2019a; Ministry of Defence n.d.). The potential effects of the weapons and the way their means of delivery work are also relatively well known. This includes other allies’ relevant capabilities, for example, the German Tornado bombers’ capability to deliver nuclear weapons (Freedman 2013, 15). This allows NATO to integrate the weapons’ potential effects in the planning of the alliance’s military defense and deterrence. The Nuclear Planning Group, founded in 1966, is the main forum to discuss nuclear issues within NATO (NATO 2022b).

As Table 1 shows, OCOCs is in a category to itself regarding NATO’s members’ will and ability (or rather lack of it) to coordinate these means through NATO.

While NATO in principle can handle defensive cyber on par with conventional means, OCOCs are even less coordinated than nuclear weapons. Contrary to the other capabil- ities, NATO as an organization likely has no knowledge of its members’ OCOCs, their effects and means of delivering it. Furthermore, NATO does not coordinate or standar- dize allies’ OCOC development or acquisition or to coordinate their use, except for the option of providing SCEPVAs through CyOC.

#### OCOCs require knowledge and prior assessment of assets – not available under NATO structures

**Jensen, Institute for Strategy and War Studies, 2022**

[Mikkel Storm, “Five good reasons for NATO’s pragmatic approach to offensive cyberspace operations”, Defense Studies, 30 May 2022, Francis and Taylor Online, 6/29/22, <https://doi.org/10.1080/14702436.2022.2080661>, GDI – LL]

\*Computer Network Attacks (CNA)

\*Computer Network Exploitation (CNE).

\*OCO - offensive cyberspace operations

\*OCOC - offensive cyberspace operations capabilities

Cyber: a young domain for offensive NATO operations

While NATO has de facto been involved in defending its member states in the cyber domain for nearly two decades, it was not until 2016 that NATO acknowledged cyber as a domain for military operations. More than half of NATO’s members had publicly declared their intent to develop offensive cyber means before NATO agreed to develop a capability to integrate such effects and began to implement a Cyberspace Operations Center, the CyOC, in October 2018 (Brent 2019; Freedberg 2018; MacKenzie 2017; Smeets 2019).

NATO’s decision to establish the CyOC to integrate offensive cyber effects in NATO led operations, is a significant and less ambitious divergence from NATO’s normal approach, which would be to coordinate offensive cyber (Rizwan and Ricks 2017). Outside the realm of OCOCs, coordination of military means in NATO operations normally involves a prior common understanding between allies of the available cap- abilities for planning purposes. At the strategic level, NATO must know which means are available to plan the ways the alliance can achieve the desired ends. At the operational and tactical level, coordination requires some level of shared command and control as well as shared information about, e.g., which weapons are used, the intended targets and the timing of the attacks in order to de-conflict with other forces engaged in the operation.

For OCOCs, however, NATO’s ambition only amounts to allow their potential inclusion in an operation, should an ally volunteer CNA-effects. No prior knowledge or assessment of available assets is collected, and no command and control exercised, except for the permission from NATO to the effect-delivering member state to execute the CNA (NATO 2020, 21).

The practical outcome is, which prior to an operation, in principle NATO staffs at the strategic and operational level will have no knowledge of what OCOCs are available to base their planning on. Broadly speaking, NATO-members will volunteer CNA- effects as they identify opportunities to support operations during the operational planning process and as operations are ongoing at the tactical level. In principle, except for the nation that delivers the CNA-effect, alliance partners will remain ignorant of, for example, which software is used, which targets are struck and when the attacks occur. Even the efficacy of the CNAs may remain known only to the member that delivers the effect.

Unclassified information on the internal negotiations in NATO on OCOCs and the CyOC is not available, but it has probably been difficult to find common ground between the 29 members NATO had at the time. The elaborate wording used by the alliance to discuss the topic could indicate that OCOs were a controversial topic. While Denmark in 2018 pledged willing to provide “cyber weapons” and “offensive cyber effects” to NATO (Danish Ministry of Defence 2018), NATO has avoided these terms. Instead NATO have compromised on the rather ungainly term “sovereign cyber effects, provided voluntarily by Allies,” or SCEPVA (Goździewicz 2019).

Adding to the diplomatic delicateness of the matter to the alliance, difficulties are exacerbated at the legal level: All NATO-members agree that international law and the rules of armed conflict apply to offensive cyber capabilities and their effects (NATO 2020, 21). However, there is no well-established NATO, let alone international, consensus on interpretation of this in practice (Taillat 2019, 33; Smeets 2021).

### Defensive cyber – coordination possible

#### Defensive cyber strategies coordination possible within NATO – follows similar coordination patterns

**Jensen, Institute for Strategy and War Studies, 2022**

[Mikkel Storm, “Five good reasons for NATO’s pragmatic approach to offensive cyberspace operations”, Defense Studies, 30 May 2022, Francis and Taylor Online, 6/29/22, <https://doi.org/10.1080/14702436.2022.2080661>, GDI – LL]

\*OCO - offensive cyberspace operations

\*OCOC - offensive cyberspace operations capabilities

NATO’s different approaches to coordination of military means

A brief comparison of NATO’s approach to integrate the effects of OCOs vis–a-vis conventional military means, nuclear weapons, and defensive cyber, gives an indication of how the four categories of military means pose different levels of challenges to their coordination by the alliance.

Conventional military means

Coordination of the use and deployment of conventional military means has long been an essential function for NATO, sometimes even influencing individual member states’ acquisitioning or discontinuation of specific military capabilities. Coordination within NATO allow nations to focus their military investments on capabilities relevant to the alliance’s plans for defense and deterrence. Hence, during the Cold War when the main threat was a Soviet invasion, European partners stood up the main part of NATO’s ground forces while the US delivered most of the strategic power projection capabilities (Shaver and Newland 1989, 12). Coordinated force development has only increased in importance with the diminishing emphasis on static territorial defense that followed the fall of the Soviet Union as members have discontinued entire capabilities (Ek 2006, 2). A prime example is how Denmark in 2004 gave up its mobilization based territorial defense, submarines and land-based air defense – key capacities for national defense – in order to focus on deployable out-of-area capabilities for missions such as the International Security Assistance Force (ISAF) in Afghanistan (Forligspartierne 2004, 9,11). On its own website, NATO elevates the role of “setting goals for national or collective development of capabilities; and facilitating national, multinational and col- lective capability development and innovation,” done through the NATO Defense Planning Process, to be a key element in the alliance’s two pillars: Interoperability and modern weapons. Coordination at this level requires that NATO has a relatively detailed understanding of its members’ military capabilities, especially the capabilities members pledge to NATO operations, readiness- or response forces. These are evaluated by NATO to assess whether they fulfil the set requirements (‘NATO – Topic: NATO’s Capabilities’ 2020; ‘NATO – Topic: Troop Contributions’ 2020).

NATO-coordination of acquisition, deployment of conventional means, etc., is of course an ideal that has never been fully realized, as demonstrated, for example, by the Turkish procurement of the Russian S-400 air defense system in 2019 or the sudden declaration by the United States in June 2020 that 9.500 troops would be withdrawn from Germany (Bennhold 2020; Marcus 2019). However, the strong reactions that followed these deviations from inter-allied coordination demonstrates that they are exactly that: deviations from an ingrained policy that NATO allies have learned to expect from each other over decades of close cooperation (Oltermann 2020; Pamuk 2019).

Defensive cyber capabilities

Regarding defensive cyber, most NATO members stood up such capabilities at the tail end of the 20th century in response to the threats that emerged along with the internet. NATO began considering coordination of defensive cyber capabilities almost two dec- ades ago in 2002 and demonstrated its ability to do so during the cyber-attack campaign against Estonia in 2007 (Caton n.d., xi; Tikk et al. 2010, 24). Acquisition of defensive cyber capabilities have been uncontroversial for individual members and NATO alike, both strategically and legally. Today, NATO has developed both doctrines and organiza- tions to develop a defensive stance in the cyber domain, with an emphasis on resilience to attain deterrence by denial rather than punishment (Burton 2015, 309). Within NATO, vital elements of defensive cyber such as response teams and threat information are shared routinely between member states (NATO 2020). Standing multilateral organiza- tions such as NATO’s Communications and Information Agency (NCIA) and NATO’s Computer Incident Response Capability (NCIRC) work every day in defense of NATO’s own systems (Ali 2014, 33). Thus, sharing of defensive cyber capabilities and information is demonstrably possible within the alliance.

### OCOCs fail – info sharing

#### OCOCs secrecy required for success effects – means no info sharing

**Jensen, Institute for Strategy and War Studies, 2022**

[Mikkel Storm, “Five good reasons for NATO’s pragmatic approach to offensive cyberspace operations”, Defense Studies, 30 May 2022, Francis and Taylor Online, 6/29/22, <https://doi.org/10.1080/14702436.2022.2080661>, GDI – LL]

\*OCO - offensive cyberspace operations

\*OCOC - offensive cyberspace operations capabilities

Five characteristics of offensive cyber that inhibit coordination

The remaining article will demonstrate why this, for good reasons, is a particular policy for OCOCs by going through inherent characteristics of this emerging military capabil- ity. The factors are arguably all subsets of characteristic #1: they arise from the individual NATO-members’ inclination to keep OCOCs secret at the “National Eyes Only” level. However, treating characteristic #2–5 individually provides better insights into how they affect NATO. The identified inhibiting factors are in this analysis taken to their theore- tical extreme in order to illustrate the argument. Of course, contextual factors may mitigate the degree to which these characteristics inhibit coordination. It is likely that the less advanced and revealing of own capabilities the OCOC in question is, and the more existential the threat the OCOC is to be deployed against is, the more likely it is that decision makers will overcome the identified inhabitations on coordinated use. Also, the informal but very real hierarchical relationship between allies, particularly between the US and the other NATO members, will likely induce individual allies to share the necessary information in some cases (Walsh 2010, 134–37).

Characteristic #1: secrecy is a precondition for effect

A conventional weapon can, in principle, be forced through an opponent’s defenses by increasing the amount of attacking platforms and/or the caliber of the weapon systems deployed if the attacker is willing to incur the costs. In contrast, many advanced OCOCs depend on secrecy to achieve their effect: they can only penetrate an oppo- nent’s defense if it has a flaw of which he is unaware (Libicki 2009, xiii, 18). To slip through an opponent’s defenses OCOCs need a technical, organizational, or procedural vulnerability that the opponent is unaware of, for example, zero-day vulnerabilities in his software or an item with internet access installed on the opponents’ system with a low security setting. It could also be physical access to his system that allows electronic or physical tampering or simply an employee in the opponent’s organization that has been identified as liable to click on phishing mails of a particular design (Taillat 2019, 370).

Regardless of the nature of the vulnerability, should the opponent become aware of it, he will be able to address it with relative ease and at a comparatively low cost. For example, by updating and patching software or hardware, limiting physical access to systems, changing passwords on electronic items on the network and training or elim- inating the above-mentioned careless employee. Therefore, OCOCs require a very high degree of operational security to retain their potential effect, as the slightest hint of their modus of deployment or their specific targets can render them impotent (Shane et al. 2017; Smith 2013, 83). The fewer who knows – the better.

While strict operational security is undoubtedly beneficial to the deployment of conventional weapons, it is, unlike advanced OCOCs, not a precondition for their ability to deliver their effect. Hence, due to the lesser risks from operational security, there is a lower threshold for sharing knowledge of conventional capabilities between allies, than for OCOCs.

The limited available information suggests that sharing even non-cyber related classi- fied information within NATO has been a longstanding challenge (Atkeson 1984; Binnendijk and Priebe 2019, 50; de Graaff 2017; Dempsey 2017; G. K. Gramer 1999, ii, 7; Seagle 2015, 565,570).

While the individual members and their national intelligence services have long histories of intelligence collection and its use, NATO does not have a lot of institu- tional experience (Seagle 2015, 565,571). NATO has had a special committee for sharing intelligence since 1952 but the organization depends on voluntary intelligence contributions from the members. There was no NATO organization for intelligence fusing until 2006, when the NATO Intelligence Fusion Center (NIFC) was stood up. Until then, members could only provide information by making national assessments releasable to NATO (Gordon 2017; Lefebvre 2003, 531). In 2017, NATO created a second institution, the Joint Intelligence and Security Division (JISD), for common intelligence analysis based on voluntary national contributions and open sources to improve the alliance’s common situational awareness (von Loringhoven 2017). Except for a few ground surveillance capabilities and airborne radars, NATO has no internal intelligence collection capabilities (von Loringhoven 2019). NATO is also unrelated to the Five-eyes, Nine-eyes or Fourteen-eyes communities that allegedly is the US National Security Agency’s unofficial designations for multilateral agreements of intel- ligence sharing with particularly trusted partners. With the Five-eyes (US, UK, Canada, Australia, and New Zealand) being the closest partners, the communities allegedly all include non-NATO members (MacAskill and Ball 2013; Reveron 2006, 460).

US concerns of allies’ ability to handle sensitive information, particularly in the cyber domain, was accentuated over NATO members’ potential inclusion of Chinese providers, for example, Huawei, in their emerging 5 G-networks. US representatives suggested that inclusion of Chinese information technology in critical infrastructure would inhibit future intelligence sharing, not only in NATO but even within the Five-Eyes community (Elmer 2019; R. Gramer and Seligman 2020; Satariano 2019).

It is important to realize that states must overcome even more constraints to share relevant information on advanced OCOCs with allies than inhibit the delicate business of sharing classified intelligence. When allies share intelligence, they can do so in a manner that does not disclose the sources and means by which the intelligence was developed. An ally can share the information that “the enemy ship will sail at midnight” without any indication of how this information was acquired and assessed as valid. Should the ally indicate the source, this may be a deceptive fabrication to deflect investigations in the true source. A famous example is how the British during WW II shared intelligence gathered by breaking the German Enigma codes, by leading allies to believe that the information had been collected through networks of spies in Germany (Cox 2014). Even with these limitations, sharing of intelligence is a delicate matter between states and allegedly rarely takes place at a significant level in multinational organizations such as NATO (Walsh 2010, 14).

As demonstrated above, and further exploited in the following characteristics below: In order to give allies a full understanding of the effects of the use of an OCOC – both to the enemy and to themselves – it is not enough to disclose the desired effect, the SCEPVA (roughly comparable to the information “The ship will sail at midnight”). Allies will need to know technical details regarding the SCEPVA in order to assess its efficacy, legality, and potential effects on own OCO.

### AT low level OCOC sharing possible

#### Even mundane OCOC info not shared within large alliances like NATO – OCOC housed in intelligence agencies

**Jensen, Institute for Strategy and War Studies, 2022**

[Mikkel Storm, “Five good reasons for NATO’s pragmatic approach to offensive cyberspace operations”, Defense Studies, 30 May 2022, Francis and Taylor Online, 6/29/22, <https://doi.org/10.1080/14702436.2022.2080661>, GDI – LL]

\*OCO - offensive cyberspace operations

\*OCOC - offensive cyberspace operations capabilities

\*Computer Network Attacks (CNA)

\*Computer Network Exploitation (CNE).

Yet not all OCOCs need to be secret at the national eyes only-level. While STUXNET was a means that reportedly required sensitive national resources to develop and deploy, some OCOCs are likely relatively unsophisticated versions of commercially available malware or conversions from, for example, criminal sources on the dark web (Falco 2012, 20). In principle, such mundane OCOCs could be fully shared and coordinated between allies, as they pose little risk to sensitive resources and are based on standard tools rather than highly vulnerable identified flaws in the opponent’s systems. However, the limited available empirical unclassified evidence, for example, from U.S. OCOs during Operation Inherent Resolve against ISIS suggests that even coordination of “trivial” OCOCs poses very significant challenges in coalitions due to high- and perhaps over-classification (Martelle 2020).

A culture of secrecy, ingrained over centuries in national intelligence services, may be a contributing factor to over-classification of even mundane, un-advanced OCOCs (Cartwright 2018). Cyber-enabled intelligence collection and means for CNA emerged naturally as a task for intelligence organizations as they expanded their activities from the electromagnetic spectrum to the Internet. In Britain, the signals intelligence service, Government Communications Headquarters (GCHQ), is responsible for OCOCs and has taken credit for OCOs against ISIS (Flemming 2018). In Denmark, the task of developing OCOCs and conducting OCOs lies with the Danish Defense Intelligence Service (Forsvarets Efterretningstjeneste n.d.).

There are excellent reasons for organizational co-location of CNE and CNA- capabilities. Besides target selection and identification of opponents’ vulnerabilities, it provides opportunities for synergy within recruitment, training, and sustainment of the human resources (Cartwright 2018). Even when separated, OCOCs often remain closely linked to the intelligence world: The US Cyber Command still shares its commanding officer with the National Security Agency (NSA) – often jokingly referred to as “No Such Agency” in reference to its reputation for secrecy (Pomerleau 2018). Also legal and constitutional concerns may keep the OCOs closely tied to the intelligence services, especially when using CNA below the threshold of armed conflict (Chesney 2019).

Regardless of causes, mundane OCOCs appear to be generally surrounded by the same secrecy as advanced or otherwise sensitive OCOCs. As the young cyber domain matures, unadvanced OCOCs may eventually be transferred from national intelligence organiza- tions to regular military forces and become an everyday part of military operations on a par with other means (Breuer 2020). The potential restraining cultural impact of national intelligence organizations on NATO’s ability to share information is, however, a topic for another article.

### OCOCs ineffective – no ally participation

#### OCOCs limited tactical and strategic effects because of uncertainty – means that allies’ mistrust of information and effects prevent coordination within NATO – too much military risk

**Jensen, Institute for Strategy and War Studies, 2022**

[Mikkel Storm, “Five good reasons for NATO’s pragmatic approach to offensive cyberspace operations”, Defense Studies, 30 May 2022, Francis and Taylor Online, 6/29/22, <https://doi.org/10.1080/14702436.2022.2080661>, GDI – LL]

\*OCO - offensive cyberspace operations

\*OCOC - offensive cyberspace operations capabilities

\*Computer Network Attacks (CNA)

\*Computer Network Exploitation (CNE).

Characteristic #2: uncertainty of effects

OCOCs have several characteristics that make their effects more uncertain than those of conventional weapons. This is true for both their immediate tactical effect and their strategic effect as a means for conflict management. The effects of conventional weapons on specific objectives depend on the laws of physics and the characteristics of the weapon and the target. They are thus well known, or can be tested in theory or practice by engineers on mathematical models or physical mock-ups. Also, physical targets change characteristics slowly over time, and there are often physical indicators that can be observed from afar – that is, if an opponent’s command and control bunker gets an additional layer of concrete or new anti-aircraft weapons are deployed around it.

This is not the case with advanced OCOCs’ effect on their intended objectives. The specific targets are unique combinations of software and hardware that are run by specific operational procedures. As described above, any change in software, hardware, or procedures (e.g. passwords) may render impotent an OCOC designed to overcome the prior combinations and their identified vulnerabilities. In addition, changes may not be obviously apparent to an external observer, who thus will have no warning about the change. An attacker can only design his OCOC based on the latest and best intelligence, until its actual use.

Therefore, there will always remain a level uncertainty about to which degree the OCOC will deliver its desired effect, if at all. Thus allies, whose conventional military operations may depend on the successful execution of an ally’s CNA (e.g. to temporarily render air defenses inoperable in order to allow friendly aircraft to operate in the opponent’s airspace) face a dilemma whether or not to accept a risk. To assess whether the level of uncertainty to their planes is acceptable, the allies need comprehensive knowledge on how the enabling CNA is to be conducted, as well as the available information on the enemy systems on which the CNA is based (Cartwright 2018). However, as discussed above, the ally providing the CNA has a strong incentive not to share this information. This leaves the CNA-dependant allies either to take the CNA-providing ally’s word for the CNA’s efficacy against the enemy’s air defenses – or to find alternative means to ensure the effect, e.g. a conventional attack. The likelihood of the latter outcome likely increases with the potential consequences of failure to the allies depending on the CNA’s effect (Cartwright 2018).

#### Even if some incentives emerge to use OCOCs within NATO, coordination obstacles will continue

**Jensen, Institute for Strategy and War Studies, 2022**

[Mikkel Storm, “Five good reasons for NATO’s pragmatic approach to offensive cyberspace operations”, Defense Studies, 30 May 2022, Francis and Taylor Online, 6/29/22, <https://doi.org/10.1080/14702436.2022.2080661>, GDI – LL]

\*OCO - offensive cyberspace operations

\*OCOC - offensive cyberspace operations capabilities

\*Computer Network Attacks (CNA)

\*Computer Network Exploitation (CNE).

The findings raise the question of how useful OCOCs are to NATO members – primarily the smaller members – if OCOC’s use within the framework of the alliance potentially requires them to share more sensitive information with allies than they are comfortable with. The discussion has so far avoided the obvious fact that NATO’s individual members have different characteristics – particularly stra- tegic wherewithal – that influences the level to which they can expect other members to accept their volunteering of SCEPVAs. Likewise, to which degree NATO-members will have to disclose sensitive information in order to be allowed to provide SCEPVAs, or can expect forgiveness from other members should they “go rouge” and conduct CNA without NATO’s knowledge or consent.

The US has a dominant status within the alliance (Jakobsen 2014, 61; Lake 1999, 171). This likely raises US expectations of not having to ask before using SCEPVAs on behalf of NATO or be forgiven if they do. At the opposite end of the power scale, a small member such as Denmark would likely hesitate to use OCOCs unilaterally, historically preferring only to wield military power in coalitions. If asked formally or informally by the US whether in NATO or indeed in any coalition of the willing with the US, Denmark would likely also find it problematic to refuse to disclose sensitive information regarding a suggested SCEPVA. Not least because the primary effect of the SCEPVA for Denmark would rarely be the first-order effect on an enemy, but rather the second-order effect to gain prestige with the US to strengthen the transatlantic relationship and military guarantee for Denmark’s security (Jakobsen et al. 2016). Such disclosure would be painful though, and small NATO-members would probably attempt to limit them to the bilateral level – likely with the US as the second party.

However, while NATO’s individual members may be expected to generally try to accommodate US’ preferences, there is no automatic causality. Choices will vary from case to case based on the individual member’s understanding of risks and benefits. In the cyber domain, for example Germany’s, UK’s and Denmark’s initial reluctance to deny Huawei access to their telecommunication infrastructure are examples of NATO-allies that weigh other issues higher than US requests (Barnes and Satariano n.d.; R. Gramer and Seligman 2020; Mouritzen 2020; D.E. Sanger et al. 2020).

Conclusion: the SCEPVA-doctrine is a pragmatic mitigation of OCOCs’ dilemmas

This article has explored the question of the degree to which the outlined char- acteristics of OCOCs inhibit NATO’s ability to coordinate them.

Today, most NATO members consider integration of OCOCs in their military operations. As demonstrated, NATO’s members have legitimate national interests in shrouding these capabilities in secrecy. Apparently, this currently makes sharing and coordination of OCOCs an insurmountable challenge for NATO.

However, this analysis has taken the outlined difficulties of coordinating OCOCs to their theoretical extremes. To invoke Clausewitz, war – including CNA – is never an isolated act and extremes are moderated by external factors (Clausewitz 1918, 27). Hence, real-world inhibitions to share information will likely be moderated by several factors.

The threshold for willingness to share information on CNA or accept risks from allies’ offered SCEPVAs may remain constant, but the incentive to overcome it likely varies with the external threats to the alliance. All other things being equal, NATO members’ willingness to share information will likely rise with the severity of a crisis at hand, facilitating the use of SCEPVAs and perhaps paving the way for more ambitious coordination. Prior to 2022, the external pressure on NATO was relatively low. The Russian attack on Ukraine in February 2022 demonstrably infused NATO’s members with a renewed sense of urgency and set in motion alliance-strengthening initiatives, such as increased military spending and forward deployments of troops and materiel (Shapiro 2020; Detsch and Gramer 2022). Possibly, the same sense of urgency has increased the willingness to share infor- mation or accept risks if NATO should request the members to provide effects through CNA.

Also, as the cyber domain matures, the willingness to share could become more dependent on the level of intelligence assets and cyber capabilities at risk – that is, dependant on how advanced and specifically tailored the OCOCs in question are. As stated above some means are very sensitive, some are more mundane. However, currently most OCOCs appear to be highly classified regardless of their actual sensitivity, meaning that the NATO-members’ willingness to share is lower than the actual means themselves justify. As military use of OCOCs matures over time in the sense that it becomes more ingrained in everyday operations and moves partly out of its current realm of top secret, national eyes only-classification, may NATO become able to coordinate some of its member’s OCOCs.

Regardless, due to the inherent characteristics of cyber weaponry, the member states’ advanced OCOCs means will likely remain outside NATO coordination. At some point, some NATO members will likely conduct CNAs without coordination with allies or perhaps limit the coordination to bilateral consultations between the CNA-conducting ally and NATO’s dominant member, the US.

### OCOCs – escalation risk

#### Impact of offensive cyber capabilities risk escalation that spirals – means NATO allies will prefer conventional responses

**Jensen, Institute for Strategy and War Studies, 2022**

[Mikkel Storm, “Five good reasons for NATO’s pragmatic approach to offensive cyberspace operations”, Defense Studies, 30 May 2022, Francis and Taylor Online, 6/29/22, <https://doi.org/10.1080/14702436.2022.2080661>, GDI – LL]

\*OCO - offensive cyberspace operations

\*OCOC - offensive cyberspace operations capabilities

\*Computer Network Attacks (CNA)

\*Computer Network Exploitation (CNE).

Added to the resulting insecurity and ambiguity comes the lack of human experience at the present point in history. The general strategic effect of offensive cyber capabilities on the international system in peace, crisis and war is presently only beginning to be understood. Hence, their use as a means for controlling escalation in crisis and war is to a large degree a question of assumptions and educated guesses on behalf of a potential attacker. This makes the use of OCOCs as signals to an opponent in a crisis even more uncertain than signaling with tradi- tional military means and hence escalation harder to control (Cavaiola et al. 2015, 89; Nye and Joseph 2016, 49). Again, these factors are exacerbated by the incentive to keep OCOs secret from allies and the uncertainty of the actual effect of a CNA. While the effects following from characteristic #2 – uncertainty of efficacy and unintended effects caused by the secrecy surrounding allies’ OCOCs – is not an argument against collaboration amongst allies, it is a strong incentive for NATO-allies to prefer conventional alternatives to SCEPVAs in NATO operations.

#### Risk of escalation creates obstacles to allies’ participation – and international legal uncertainty decreases participation because NATO members differ in their interp of legal use of OCOCs

**Jensen, Institute for Strategy and War Studies, 2022**

[Mikkel Storm, “Five good reasons for NATO’s pragmatic approach to offensive cyberspace operations”, Defense Studies, 30 May 2022, Francis and Taylor Online, 6/29/22, <https://doi.org/10.1080/14702436.2022.2080661>, GDI – LL]

\*OCO - offensive cyberspace operations

\*OCOC - offensive cyberspace operations capabilities

\*Computer Network Attacks (CNA)

\*Computer Network Exploitation (CNE).

In addition to the uncertainty on whether contributed CNAs will have less than the desired effect, there will sometimes be uncertainty whether the CNA will have more than the desired effect, either directly or as collateral damage. The CNA may have undesirable effects, perhaps by effecting third parties, by being unintentionally escalatory or by delivering effects that are debatable according to international law. Again, allies to a state that conducts CNAs must have knowledge of the deployed OCOCs and the targets to assess its effects. Their alternative is to take their ally’s word that they will not be participating in operations involving legally questionable or plainly counterproduc- tive OCO.

Legal issues is a more pronounced problem with CNAs than with conventional means, as there are no internationally agreed upon interpretation on what constitutes the legal use of CNAs in international conflict, not even within NATO. As stated above, SCEPVAs need to be legal according to the delivering ally’s interpretation of International Law (NATO 2020, 21) – but this may differ from other NATO-members’, opening up an assortment of legal problems in case NATO decides to use CNAs (Taillat 2019, 373; Jacobsen and Jeppe 2017, 7; Smeets 2021, 3). Even though disputable legal effects of a SCEPVA will formally be the responsibility of the executing member, other members of NATO may be held responsible at the political and strategic level. Having noted this very serious inhibition, legal aspects of coordinated use of OCOCs in NATO will not be developed further here.

### OCOCs Fails – military and intelligence divisions within NATO

#### Deconfliction of military and intelligence goals in OCOCs hard at national level – fewer incentives for deconfliction within NATO

**Jensen, Institute for Strategy and War Studies, 2022**

[Mikkel Storm, “Five good reasons for NATO’s pragmatic approach to offensive cyberspace operations”, Defense Studies, 30 May 2022, Francis and Taylor Online, 6/29/22, <https://doi.org/10.1080/14702436.2022.2080661>, GDI – LL]

\*OCO - offensive cyberspace operations

\*OCOC - offensive cyberspace operations capabilities

\*Computer Network Attacks (CNA)

\*Computer Network Exploitation (CNE).

Characteristic #3: conflicting priorities between offensive cyber effects and cyber espionage

The vulnerabilities exploited when conducting CNA may well be the same vulnerabilities that are used to conduct CNE. Successful and continuous intelligence collection depends on discretion and the target of the collection being unaware of the vulnerability exploited. A CNA conducted via such a vulnerability will likely draw the opponents’ attention and eventually result in its discovery and elimination. This will render future intelligence collection from that venue impossible. Thus, there can be a conflict of interest between “cyber spies” and “cyber warriors” that has to be de-conflicted before a CNA is carried out. This inherent need to decide which is more important, immediate CNA-effects or future intelligence collection opportunities, is probably one of the reasons why the US Command for Military Cyber Operations, and NSA, the intelligence service responsible for technical collection, still have a common commanding officer after years of con- templation of separating the two institutions (DoD n.d.). By having the same person in charge of both CNA and CNE, the competing priorities can be decided within the same organizational framework with full knowledge of the technical and tactical details required to make a full assessment of the effects and risks involved. Even so, the limited available information on historical OCO suggests that inter-organizational de-confliction just within the US is problematic (Loleski 2019, 123; USCYBERCOM 2016).

It is reasonable to assume that the added layer of complexity of de-conflicting use of identified flaws in the opponent’s systems with allies is even more problematic than sharing other SCEPVA-related information. Such de-confliction may include detailed disclosures of highly sensitive means, methods and operations regarding both CNA and CNE capabilities. Hence, this will be very difficult to carry out on a bilateral basis, let alone in a multilateral alliance. To de-conflict SCEPVAs, allies may have to disclose highly sensitive information to other alliance members – which they will have a strong inclination against. NATO has, as mentioned earlier, reportedly had challenges sharing intelligence. This suggests that the more likely outcome is that de-confliction will be omitted, and NATO allies will have to accept the risk that a SCEPVA could shut down some of their intelligence collection sources. Intelligence collection means, technical and otherwise, are the crown jewels of intelligence services, and while the collected informa- tion or intelligence-based thereon occasionally is shared, means are kept secret from friends as well as foes. As is the case with the other inhibitions to coordination derived from over-classification of mundane OCOCs along with the actual tailored means, this hindrance could be lessened if NATO members distinguished between the two sorts and treated them differently (Cartwright 2018).

### OCOCs – burning OCOCs disincentive

#### Limited investment in OCOCs – no incentive to prioritize sharing effects that burn ococs for future use

**Jensen, Institute for Strategy and War Studies, 2022**

[Mikkel Storm, “Five good reasons for NATO’s pragmatic approach to offensive cyberspace operations”, Defense Studies, 30 May 2022, Francis and Taylor Online, 6/29/22, <https://doi.org/10.1080/14702436.2022.2080661>, GDI – LL]

\*OCO - offensive cyberspace operations

\*OCOC - offensive cyberspace operations capabilities

\*Computer Network Attacks (CNA)

\*Computer Network Exploitation (CNE).

Characteristic #4: competing priorities for the use of an offensive cyber capability

Once developed, conventional weapons, e.g. bombs, of the same model can be used again and again until they become obsolete. In contrast, advanced OCOCs can only achieve effects until the vulnerability they exploit is eliminated, which, as described above, is likely to happen shortly after it is exposed (Smeets 2018a, 16). Hence, advanced OCOCs are in some sense not re-usable or at least highly ephemeral, once deployed.

Bearing this characteristic in mind, consider that allies, who possess OCOCs utilizing the same identified vulnerability, may have different priorities regarding which targets to use the capability against. As was the case with de-confliction of intelligence collection versus CNA, de-confliction in alliances of target priorities when “burning” OCOCs and disclosing the opponent’s vulnerabilities with CNAs will require sharing highly sensitive information. This will very likely inhibit the de-confliction process. Alternatively, allies must accept the use of OCOCs without this knowledge, accepting the risk of some of their own arsenal of OCOCs becoming obsolete, as the capabilities will likely become impotent shortly after their first use.

### OCOCs bad – reuse against US and allies

#### OCOCs once used and info about effects shared risk reuse by adversaries and criminals against allies – decreases incentives to share cyber effects and OCOCs

**Jensen, Institute for Strategy and War Studies, 2022**

[Mikkel Storm, “Five good reasons for NATO’s pragmatic approach to offensive cyberspace operations”, Defense Studies, 30 May 2022, Francis and Taylor Online, 6/29/22, <https://doi.org/10.1080/14702436.2022.2080661>, GDI – LL]

\*OCO - offensive cyberspace operations

\*OCOC - offensive cyberspace operations capabilities

\*Computer Network Attacks (CNA)

\*Computer Network Exploitation (CNE).

Characteristic #5: Risk of offensive cyber means being used against allies and third parties

However, OCOCs are re-useable in ways that conventional munitions are not. After a bomb dropped on an opponent detonates, the opponent can’t pick it up, perhaps re- engineer it, copy the bomb or its new versions endlessly and then use it against the original attacker, his allies or third parties – or sell it to criminals at the dark web. With some OCOCs, you can. In some cases, a victim of a CNA will be able to find, extract and re- engineer the malware and potentially use it against, for example, the original attacker, its allies, or third parties outside the current conflict (Taillat 2019, 375). To give a famous example, the US and Israel allegedly deployed STUXNET in 2009–10 as a CNA to sabotage of Iranian centrifuges. By September 2010 elements of the software had already been adapted by criminals and used to attack third parties (Falco 2012, 33–34). The same is the case when OCOCs are lost or stolen. Sometime in or before 2013, a number of OCOCs developed by the NSA’s hacking group, Tailored Access Operations, was lost (Shane et al. 2017). Regardless whether this was due to external state sponsored CNE or an insider attack along the lines of the 2013-Snowden-breach, the lost OCOCs have since been used against targets in the US, NATO allies, and third parties, for example, Ukraine in different guises. Russia conducted the 2017 NotPetya CNA on critical economical infrastructure in Ukraine based on flaws identified in the tools lost by NSA. It spread uncontrollably to other countries and caused damage to civilian companies in the west for more than 800 million USD (UK NCSC 2018). Prior to that, in 2016, North Korea used them for extortion attempts in the Wannacry CNA that infamously paralyzed several British hospitals for days and caused costly disruptions in many other countries (Shane et al. 2017). Iran has also been identified as a likely user of the lost OCOCs (Symantec 2018). Lately, criminals have used the tools to disrupt and degrade entire cities’ informational infrastructure and holding municipalities for ransom, for example, in Baltimore, which suffered the effects of such an attack for months in 2019 (Perlroth and Shane 2019).

Hence, by conducting a CNA, an alliance member will let loose an OCOC on the Internet for all to eventually find and examine. This may eventually add the means or redesigned versions of it to opponents’ cyber arsenals, as well as the arsenals of capable non-state actors, such as criminals (Robinson et al. 2015, 81). Thus, as part of the alliance’s coordination efforts the CNA-providing ally should consider warning allies and perhaps even third parties, for example, about which means have been used or which vulnerabilities have been exploited (Baram 2018). However, again the tactical value of keeping details about OCOCs and identified flaws in software classified will provide a strong incentive against such coordination. For example US authorities waited years to warn US entities in 2017 and 2019, respectively, of security flaws that were left vulnerable after the CIA lost control of a number of OCOCs in 2016 (Wyden 2020).

### OCOCs fail + escalation – intel sharing

#### Intel sharing required for effective OCOCs limit utility – and risk of escalation if intel is inaccurate undermines incentives for sharing within NATO

**Jensen, Institute for Strategy and War Studies, 2022**

[Mikkel Storm, “Five good reasons for NATO’s pragmatic approach to offensive cyberspace operations”, Defense Studies, 30 May 2022, Francis and Taylor Online, 6/29/22, <https://doi.org/10.1080/14702436.2022.2080661>, GDI – LL]

\*OCO - offensive cyberspace operations

\*OCOC - offensive cyberspace operations capabilities

\*Computer Network Attacks (CNA)

\*Computer Network Exploitation (CNE).

The uncertainties regarding the potential technical and tactical efficacy of SCEPVAs are increased by the fact that collection of intelligence on potential targets has to be done in a discreet, preferably clandestine, manner. This is in order not to alert the opponent and cause him to take actions, for example, implement technical changes that may render the CNA under preparation impotent (Cavaiola et al. 2015, 87). The necessary collection of intelligence to prepare tailored CNA may involve highly classified national means, methods, and capabilities. These could be jeopar- dized by sharing information on the intended OCOCs or CNA-targets with allies. Along with the need for operational security and secrecy described above, this risk to intelligence capabilities further constrains an ally’s incentive to share information on OCOCs with alliance partners.

As a strategic means, OCOCs are in some regards more challenging as means of escalation control and crisis management for alliances than conventional means. One major difference is the ambiguous nature of CNA. Unlike conventional weapons, CNA will always leave the victim of the attack in some level of uncertainty regarding attribu- tion, and whether it has realized all the ways in which it has been attacked (Libicki 2009, 92; Rid and Buchanan 2015, 11). The US initial reactions to the Solar Winds attack, attributed tentatively to Russian intelligence, provide ample evidence of the insecurity that follows the discovery of a deep penetration of critical systems (Fireye 2020; David E. Sanger and Perlroth 2020).

### AT: US contributions key to offensive cyber operations

## Resiliency

### AT: US contributions key to resiliency

# CPs

## EU

### \*\*solvency\*\*

### Solvency - Baltic Approach

#### EU and US adoption of Baltic Approach solves data governance and cybersecurity prioritization

**Selga, 2021**

[Eriks, Digital Innovation Baltic Fellow with the Transatlantic Leadership team, Visiting Researcher at the Latvian Institute of Foreign Affairs, Associate Scholar at the Foreign Policy Research Institute; “Building Common Ground in Transatlantic Cybersecurity – A Baltic Approach” The Center for European Policy Analysis August 27 2021 <https://cepa.org/building-common-ground-in-transatlantic-cybersecurity-a-baltic-approach/> accessed 6/9 GDI-tm]

Executive Summary

• As sectors continue to grow more dependent on data flows, cybersecurity threats are becoming a bigger priority for the United States and the European Union (EU). Preventing cybersecurity breaches is becoming increasingly important to critical sectors and critical functions across the transatlantic.

• Data governance frameworks between the United States and the EU diverge significantly, with fundamental differences in approaches to data architecture, data protection, law enforcement data sharing, cyber interventions, and cybersecurity frameworks.

• Differences in data governance lead to growing cybersecurity risks in the transatlantic, caused by different cybersecurity risk assessments, cybersecurity incident reporting standards, and information sharing networks.

• The Baltic approach ensures that all cybersecurity information funnels through a forum of all relevant public, private, military, and civilian sector stakeholders.

• By establishing an international cybersecurity council for critical functions, the United States and the EU set a shared scope for threat collection, and a forum for sharing threats.

• Cybersecurity coordination should be advanced as a priority under the U.S.-EU Trade and Technology Council working groups.

• Civilian and military cybersecurity expertise and capacity should be conflated. The EU proposal for a Joint Cyber Unit would establish a unit that can become a European representative to the United States.

### \*\*net benefits\*\*

### Escalation net benefit – general cyber

#### Turn - NATO efforts misperceived and risks escalation, especially true of offensive cyber efforts or hybrid warfare deterrence

Jacobsen, 2022

[Jeppe, PhD candidate Danish Institute for International Studies and the University of Southern Denmark and former coordinator of Denmark’s cyber diplomacy in European Union and NATO, "Cyber Offense in NATO: challenges and opportunities", International Affairs, Vol. 97, Issue 3, May 2021, https://academic.oup.com/ia/article-abstract/97/3/703/6205395, accessed 7/1/22, GDI-cc]

This article has pointed to several challenges to the integration of military cyber effects in NATO operations, and has argued that even if the integration is successful, it will not add to the alliance’s deterrence posture. Importantly, the fact that CYOC does not send a strong signal to adversaries such as Russia does not mean that it is a waste of time. Far from it. As both conventional militaries and paramilitary groups are increasingly dependent on civilian networked technolo- gies, the ability of NATO to disrupt, deny, degrade or destroy enemy networks through sovereign cyber effects—even if these amount only to temporary annoy- ances—will become more relevant in the years to come. This, of course, does not mean that conventional kinetic or electromagnetic capabilities will become redun- dant. Rather, cyber effects offer a substitute in case the intended target cannot be reached with conventional capabilities, and a supplement that works alongside conventional operations as persistent annoyances of enemy networked devices. The latter, however, demands an agile CYOC that provides member states with broad initial mandates and facilitates quick decision-making and rapid approval when member states stand ready to deliver even minor cyber annoyances.

Furthermore, the article has argued that NATO and its CYOC should not seek to coordinate additional offensive cyber efforts to deter hybrid activities below the threshold of armed conflict. If an organization that is perceived by its main adversary primarily as a military organization engages in active cyber-defence measures and persistent cyber engagements outside of military confrontation, then the risk of escalation increases. This is because every potential NATO-initi- ated cyber activity in foreign networks is likely to be perceived through a military lens and thus to be (mis-)interpreted as an attack in the making. In fact, active cyber-defence measures in foreign networks and use of cyber means below the threshold of armed conflict to pursue political interests internationally are part of our current reality. Intelligence agencies know this to be a fact, and they live by it every day.

#### NATO ineffective cyber deterrent and increased focus on cyberspace undermines intelligence norms necessary for de-escalation

Jacobsen, 2022

[Jeppe, Ph.D. candidate at the Danish Institute for International Studies, "Cyber Offense in NATO: challenges and opportunities", International Affairs, Vol. 97, Issue 3, May 2021, https://academic.oup.com/ia/article-abstract/97/3/703/6205395, accessed 7/1/22, GDI-cc]

Deterring cyber activity below the threshold of collective defence

‘Hybrid’ has become a popular concept when describing the current threat environment. While discussions over the definition, novelty and usefulness of the concept continue, there seems to be agreement that, when used to qualify ‘threat’ or ‘warfare’, ‘hybrid’ refers to the blurring of the distinction between military and civilian, often in relation to the mixture of instruments used to obtain political objectives.62 NATO’s attempt to deter military and paramilitary instruments from being deployed has already been touched upon above. As a primarily military alliance, however, NATO is facing difficulty in addressing the instruments that are used deliberately to stay below the threshold of collective defence.

NATO has not been able to deter the perpetration of random ransomware incidents, election interference and targeted propaganda campaigns through hacks and leaks, or industrial cyber espionage and intrusion into critical infrastructures. The alliance’s conventional capabilities are not credible (proportional) responses to such malicious cyber activity. Thus, it has responded only by ‘naming and shaming’, and by expressing encouragement to member states to enhance the resil- ience of their networks.63 These responses, however, have yet to prove effective in halting the malicious cyber activity conducted below the threshold of collec- tive defence.64 And the introduction of SCEPVA is not likely to change that; the integration of cyber effects is tied to NATO military operations only. While NATO member states are already compelled to maintain a level of cooperation in collective defence (article 3), and to consult together whenever any of them feels that its territorial integrity, political independence or security is threatened (article 4), NATO—with or without integrated cyber effects—is not an alliance designed to deal with non-military threats from a peer competitor.

The question then arises: does the lack of capacity to deter non-military hybrid cyber activities suggest that it is time for NATO to renegotiate the scope and substance of its collective defence clause?65 When it comes to cyberspace, the next section expresses scepticism about expanding NATO’s role. It addresses the escala- tion risk associated with having NATO, an organization that has refocused its attention on a more traditional military threat, become a more active player below the threshold of collective defence. It argues that a more active stance outside military confrontation risks undermining the intelligence norm that currently dominates in cyberspace—a norm whereby state activity in foreign networks is not considered escalatory.

### Escalation net benefit - NATO cyber offense specific

#### NATO integration of offensive cyber doesn’t solve deterrence and increases risk of escalation

Jacobsen, 2022

[Jeppe, Ph.D. candidate at the Danish Institute for International Studies, "Cyber Offense in NATO: challenges and opportunities", International Affairs, Vol. 97, Issue 3, May 2021, https://academic.oup.com/ia/article-abstract/97/3/703/6205395, accessed 7/1/22, GDI-cc]

\*SCEPVA – sovereign cyber effects Provided Voluntarily by Allies

\* CYOC - Cyberspace Operation Centre

The article makes three arguments in support of the overall argument that NATO will (and should) continue to play only a limited offensive role in cyber- space. First, it identifies four distinct cyber effects from the current debates on major cyber incidents presented in the cyber-conflict literature. This is done in order to assess the operational challenges and possibilities for successful integra- tion of sovereign cyber effects in NATO operations, also known as SCEPVA.8 As cyber effects are often costly in time and resources to develop, difficult to predict and verify, and involve a risk of confliction, it is argued that the types of offensive cyber operations that are highly destructive and specialized, with a view to enabling other (kinetic) military effects, are the most difficult to integrate. In contrast, less complex disruptions used to persistently annoy and confuse adversaries hold more promise. In order to work in NATO, these effects require more flexibility in the way CYOC sends requests to and interacts with the member states.

Second, in the light of the renewed scholarly attention being given to NATO’s capacity to deter Russia, the article unpacks and assesses the suggestion that a centre for integrating offensive cyber effects contributes to NATO’s deterrence posture.9 It assesses the addition of cyber effects to NATO’s operational toolbox in the light of the (hybrid) threat environment which is currently being articulated in NATO, and argues that such integration adds little to the existing deterrence posture. NATO’s superior conventional capabilities—with or without cyber effects—already threaten punishment to adversaries who may consider invading allied countries. Yet CYOC and the alliance as a whole do not deter the more frequent (hybrid) cyber activity against member states that does not reach the threshold of armed conflict.

To elaborate on this argument, the article addresses, thirdly, the question of misinterpretation and escalation in cyberspace. Despite being potentially counter- intuitive to those scholars who advocate a stronger NATO deterrence posture, the limited offensive role of NATO in cyberspace and the alliance’s inability to deter the majority of malicious cyber activity against member states is not necessarily a problem. In fact, the article argues that the reason why we have yet to experi- ence serious misinterpretation in cyberspace is that most states’ cyber activities seem implicitly to accept an intelligence norm in cyberspace that embraces acting in legal grey zones and staying under the threshold of armed conflict. This norm has offered an additional option on the escalation ladder below armed attack, but its continuation is contingent on an intelligence logic—and not a military logic—being the dominant way of thinking in cyberspace. As the current strategic adaptation represents a return to a more conventional military way of thinking, NATO’s move to present a dominant military force in cyberspace risks under- mining the status quo—which, so far, has avoided rapid escalation.

### EU – key to revitalized liberal international order

#### US leadership not key to new world order -decentralized with EU leadership key

**Zelikow,** Professor of History at the University of Virginia and Executive Director of the 9/11 Commission, **2022**

[Philip, “The Hollow Order Rebuilding an International System That Works” Foreign Affairs July/August 2022 <https://www.foreignaffairs.com/articles/world/2022-06-21/hollow-order-international-system?utm_medium=social&utm_campaign=tw_daily_soc&utm_source=twitter_posts> accessed July 4 GDI-TM]

IN IT TOGETHER

It may be easy, and perhaps natural, for the would-be architects of the new system to organize it around Washington. But that would be a mistake. The enemies of this new order, united by their resentment of the United States, will seek to discredit it as just another effort to dominate global affairs. For this new order to be viable, it must be conceived in such a way that the charge is false.

The new order must also be decentralized to be effective; the resources and wisdom needed to solve many vexing problems are not concentrated in the United States. For instance, on the enormous issue of defining rules for a digitized world, Washington has been confused and passive, despite—or perhaps because of—its dominance in such commerce. It is the European Union that has led the way. The EU’s General Data Protection Regulation, its Digital Services Act, and its Digital Markets Act created the standards that influence most of the world, including the Americas. Decentralized leadership has also proved critical to responding to Russia’s aggression in Ukraine. The nucleus of the emerging pro-Ukraine coalition, for instance, is not just the United States but the entire G-7, including the European Commission. South Korea and Australia should be invited to join this coalition as well.

## US unilateral/Cyber Command

### \*\*do the plan\*\*

### Unilat Solves – better than NATO

#### CP – US Cyber Command solves better than NATO cyber actions – defend forward and intel norm basis

Jacobsen, 2022

[Jeppe, Ph.D. candidate at the Danish Institute for International Studies, "Cyber Offense in NATO: challenges and opportunities", International Affairs, Vol. 97, Issue 3, May 2021, https://academic.oup.com/ia/article-abstract/97/3/703/6205395, accessed 7/1/22, GDI-cc]

The large overlap between intelligence collection and attack in cyberspace makes it difficult to send clear signals to adversaries, in terms of either capabilities or intentions. When a foreign entity is moving around in a network, is it then about to start a military operation? Is the activity part of a reconnaissance mission? Is it political or economic espionage? Is it active defence? The difficulty of answering these questions has created much nervousness among cyber-conflict experts. Ben Buchanan, for example, has shown how defensive hacking or intelligence-gather-ing in cyberspace is easily misinterpreted as aggressive behaviour.66 Why, then, have we not experienced serious misinterpretation and escalation in cyberspace?

One way to explain this is through the existence and dominance of a largely unspoken but widely accepted norm. For decades, the predominant actors in cyberspace have been intelligence agencies; and the norms that characterize inter- actions between intelligence agencies are not primarily concerned with military concepts such as conflict escalation and deterrence.67 In the world of intelligence agencies, success is not about keeping a distance between oneself and the adversary by signalling one’s intentions and capabilities. It is about being able to outma- noeuvre adversaries in a space of constant contact.68 There are always risks, and the work usually takes place in legal grey zones where a clear distinction between war and peace is not the guiding principle. This is an arena where the opportunity to annoy, cheat and delay opponents is taken when it arises. **In short, espionage and counter-espionage do not fit well with the thorough military operational planning that characterizes NATO operations**. Intelligence operations, on the other hand, fit perfectly with a dynamic cyberspace where anonymity is easy to achieve and uncertainty a constant condition.69 The states that embrace cyber- space as a domain where the intelligence norm dominates are able to use a broader array of tools to pursue or respond to various foreign political objectives than only those that relate to military operations.

In its 2018 ‘vision’, the US Cyber Command built implicitly on the dominant intelligence norm. Here, the objective is to become more agile and act as close to the adversary as possible (‘defend forward’).70 The United States considers ‘constant contact’ and ‘persistent engagement’ as the necessary guiding principles to achieve superiority in cyberspace and to take full advantage of the broader potential for pursuing its political objectives through cyberspace. During the 2018 US midterm elections, for example, the US Cyber Command worked closely with the NSA to disrupt servers operated by the Russian Internet Research Agency aiming to spread fake news and stir up tension in the United States.71 More recently, the US Cyber Command responded with various cyber effects against Iran after the Iranian Revolutionary Guards apparently placed mines on ships in the Strait of Hormuz.72 These practices illustrate that, for the United States, cyber effects provide political options when one does not want to escalate existing tensions into military confrontation. Defensive coordination between allies through CYOC supports such defensive use of cyber effects, increasing the possibility that US Cyber Command will be allowed to ‘defend forward’ and work persistently through allied networks.73 A more cyber-active NATO, however, risks being counterproductive to the ambition to ‘defend forward’ through allied networks.

Unintended conflict escalation from ongoing cyber activity is mainly a risk if military analysts—in a strategic environment with heightened attention to military confrontation—ignore the dominant intelligence norm. If that happens, it becomes more likely that ‘persistent engagement’ and active cyber defence will be misinterpreted as military preparation, armament or the initial phase of an attack**. If NATO, an organization that has publicly returned to its original raison d’être of deterrence and collective defence, becomes the entity that coordinates cyber effects below the threshold of armed conflict, then the likelihood increases that Russia misinterprets these effects as escalatory and acts accordingly. In other words, a more active NATO in the current strategic environment increases the risk that the existing intelligence norm will be undermined and replaced by a more militarized norm.**

This does not mean that states that face hostile hybrid activities below the threshold of armed conflict will be left alone. Intelligence cooperation between allied countries does exist, and threat information is occasionally shared. In addition to the current political collaboration facilitated by NATO to improve network security and resilience, the EU is engaging in similar civilian activities, as well as developing and implementing a cyber-diplomatic toolbox to create a common basis for responding to a variety of malicious activities against member states. Further strengthening the political partnership between the EU and NATO is thus the most appropriate way forward to avoid further militarization of cyber- space.

Sustaining the intelligence norm as the dominant norm is not without potential problems. Openly embracing the fact that cyberspace is a domain in which intel- ligence agencies are constrained only by domestic laws, and where takedowns of servers in foreign countries are not necessarily perceived as serious breaches of sovereignty, is likely to lead to an increase in the exploitation of IT vulnerabili- ties in commercial software used in both enemy and allied networks. For smaller states, this could increase the risk of retaliation by larger adversaries, and it could increase the risk of divisions between allies—divisions that are not aligned with the United States’ political ambition to use cyber coordination in NATO as part of its attempt to ‘defend forward’.74 More exploitation could also ultimately make cyberspace less free, less open and less secure, rendering civilian populations more susceptible to cybercrime, surveillance and disruptions of everyday services.75 This is why some states, NGOs and private corporations such as Microsoft continue to promote norms that emphasize restraint on the part of states’ intelligence agencies and militaries in cyberspace, and why other states promote more sovereign control of cyberspace.76

### \*\*Cyber signaling\*\*

### US Unilateral CP – clarify policy solvency

#### US unilateral policy clarification on cyber policy – especially when delegated decisionsmaking – decreases risk of escalation

**Lonergan**, assistant professor at the Army Cyber Institute at the US Military Academy, and **Lonergan**, senior director in the Cyber, Risk & Regulatory Practice at PricewaterhouseCoopers, **2022**

[Erica and Shawn, “Cyber Operations, Accommodative Signaling, and the De-Escalation of International Crises”, Security Studies, 18 Feb 2022, Taylor and Francis, accessed July 1, 2022, JCP-LL]

Finally, there are also policy implications for the United States. In gen- eral, policymakers should more systematically consider how to incorporate cyber operations into crisis-management plans and strategy, and further improve communication channels and infrastructure regarding cyber con- tingencies. Establishing or strengthening bilateral confidence-building meas- ures with rival states (especially lines of communication) could enable leaders to privately communicate about cyber operations, enhancing the US government’s ability to send clearer signals and couple action with direct, private messages.139 For example, in 2013 the United States and Russia agreed that the hotline established during the Cold War to communicate about nuclear crises, the Nuclear Risk Reduction Center, could also be used for cyber contingencies.140 During Russia’s interference in the 2016 US elec- tions, President Obama used the hotline to communicate with Moscow, reportedly to deter Russia from directly interfering in the election out- come.141 The United States lacks a comparable hotline with China to com- municate about cyber or other incidents; as of this writing, the US military held its first talks with Chinese counterparts on this topic during the Biden administration.142 US policymakers should continue to pursue efforts to establish formal lines of communication or, at a minimum, points of con- tact to facilitate communication around cyber incidents during crises.

Additionally, in 2018 US military posture in cyberspace shifted toward a more active operational presence, epitomized in the Department of Defense and Cyber Command concepts of “defend forward” and “persistent engagement,” respectively.143 However, it is unclear whether policymakers have systematically assessed how US cyber operations, particularly during times of crisis, map onto a broader signaling strategy. For instance, during the 2018 effort to protect the US midterm elections from cyber interfer- ence, it was reported that US cyber operations were coupled with private communications to Russia, including US Cyber Command sending direct (private) messages to Russian operatives.144 Especially in a context in which approval for cyber operations may be delegated down the chain of com- mand,145 there is a risk that operational activity may be mismatched with broader strategic objectives, raising concerns about strategic disintegration or the various arms of government operating at cross-purposes. Therefore, policymakers should take a more deliberate approach to cyber operations’ different uses for signaling purposes and build more institutionalized mech- anisms for communicating with adversaries during times of crisis—espe- cially for accommodative purposes or to ratchet down tensions—so that signals are neither lost in the noise nor misinterpreted.

### \*\*clarification CP\*\*\*

#### US should signal restraint in cyber operations for confidence building measures to de-escalate risk

Lonergan and Yarhi-Milo, 2022

[Erica, assistant professor in the Army Cyber Institute at West Point, and Keren, director of the Arnold A. Saltzman Institute of War and Peace Studies at Columbia University, "CYBER SIGNALING AND NUCLEAR DETERRENCE: IMPLICATIONS FOR THE UKRAINE CRISIS", War on the Rocks, 4/21/22, https://warontherocks.com/2022/04/cyber-signaling-and-nuclear-deterrence-implications-for-the-ukraine-crisis/, accessed 7/4/22, GDI-cc]

The Biden administration has been commendable in clearly and consistently communicating to Russia, and other audiences, what the United States will not do in the Ukraine crisis — like sending American forces to Ukraine or establishing a no-fly zone. In addition, the administration should be equally clear about what is off the table in cyberspace — what Jacquelyn Schneider has termed a “strategic no-first-use” policy in cyberspace. Specifically, the United States should unequivocally convey to Russia that it will refrain from taking actions in cyberspace during this crisis that would undermine nuclear stability, such as conducting disruptive cyber-attacks against early warning satellites. This is different — the opposite, in fact — from drawing “red lines” in cyberspace, which are meant to deter unwanted behavior but can often backfire. Instead, the United States should communicate where it will exhibit restraint in cyber operations — a form of confidence-building. This could be conveyed publicly through statements by administration officials, similar to statements that Biden has made about other aspects of America’s role in Ukraine. It could also be privately communicated through ongoing backchannels taking place between U.S. allies, like France, and Russia.

There are also policy implications beyond the Ukraine conflict, especially in an environment in which the United States confronts potential future crises with other nuclear powers. In particular, senior national security officials have repeatedly emphasized that China represents a “pacing challenge” for the United States, including across the nuclear and cyber realms. In fact, Gen. Nakasone recently announced the creation of a China Outcomes Group under Cyber Command and the NSA. And researchers have identified how hypothetical crises involving the United States and China could escalate along dangerous trajectories, including to the use of nuclear weapons. The consequences of misunderstanding the utility of cyber signaling in this area are significant. Therefore, policymakers must consider how to improve civil-military coordination and cohesion so that the employment of military cyber power — especially when used against sensitive adversary systems, particularly nuclear ones, during delicate periods — is not out of sync with strategic objectives. The United States should also develop a more robust effort to clarify to adversaries, including China, how it will constrain its own behavior in cyberspace specifically during nuclear crises. The potential implications of misperceptions surrounding cyber operations targeting nuclear systems during a future crisis with a nuclear-armed adversary are simply too significant.

## Advantage CP – nuclear deterrent

### CP- US NATO nuclear deterrent

#### US and NATO should change nuclear posture documents to assert first use policy and engage in more exercises to practice operational readiness

**BOWEN, 2022**

[Tyler, postdoctoral fellow in the Kissinger Center at Johns Hopkins SAIS “RUSSIA’S INVASION OF UKRAINE AND NATO’S CRISIS OF NUCLEAR CREDIBILITY” WOR April 20, 2022 <https://warontherocks.com/2022/04/russias-invasion-of-ukraine-and-natos-crisis-of-nuclear-credibility/> accessed 7/4/22 GDI-TM]

The alliance already has B61 gravity bombs deployed across five countries in Europe and deliverable by dual-capable aircraft. The United States and NATO can enhance their impact by changing the Nuclear Posture Review and the Deterrence and Defence Posture Review to stress that they reserve the ability to use nuclear weapons first. In addition, the aircraft units assigned to carry NATO’s nuclear weapons can hold more exercises to emphasize the operational readiness of those forces. If an attack by Russia looks imminent, the United States, in consultation with NATO allies, can put those forces on alert. The goal of these steps by the United States and NATO would be to emphasize to Russia the nuclear implications of an attack on a NATO country without taking steps that could cross a Russian “red line” and provoke it.

What is important here is not making sure that NATO has more tactical nuclear warheads than Russia or that they are able to stop a Russian advance on their own. NATO’s nuclear weapons would primarily have a political effect: threatening a breach of the nuclear threshold. The current arsenal of around 130 tactical nuclear weapons should be sufficient for that task.

Such an asymmetric escalation strategy is not ideal and carries great risks, but it is a product of past decisions to expand NATO without first developing real plans for the defense of new members. NATO expansion came at a time when policymakers assumed that the risk of war in Europe was low and thus did not have to think about the dynamics of great power war or escalation. Putin has disabused Western leaders of their naïveté and in the process shown himself to be aggressive and risk-acceptant in the pursuit of ambitious goals. Threatening early nuclear use in a NATO-Russia conflict may be the best way to protect Europe from Putin’s recklessness.

# DA links

## NATO Overstretch/Focus

### Non-unique – strategic concept

#### New strategic concept focus on cyber and resiliency now

**Monaghan, et al 2022**

[Sean, visiting fellow in the Europe, Russia, and Eurasia Program at the Center for Strategic and International Studies, "What Happened at NATO’s Madrid Summit?", CSIS, July 1 https://www.csis.org/analysis/what-happened-natos-madrid-summit, accessed 7/3/22, GDI-cc]

Q7: How will NATO adapt to new security challenges?

A7: A key question on the road to Madrid was how the alliance would discuss new security challenges related to space, cyberspace, hybrid tactics, climate change, and emerging and disruptive technologies (EDTs). Each receives their due in the strategic concept: after Russia, they are the first challenges listed in an overview of the strategic environment.

The most eye-catching may be cyber and hybrid threats, which “could lead the North Atlantic Council to invoke Article 5.” The commitment to resilience is also pertinent. On EDTs, NATO announced a new innovation fund to complement the “DIANA” initiative launched in April. The concept language on climate change was also ambitious: “NATO should become the leading international organisation when it comes to understanding and adapting to the impact of climate change on security.”

### Cyber – limited military resources

#### Carefully employing military cyberspace capabilities prevents further data-breaches

**Păunescu, 2021**

[Dragoș-Mihai, PnD in International relations at the Carol I National Defence University, “NATO’S ENCOUNTERS IN THE CYBER DOMAIN”, 11/9/2021, https://revista.unap.ro/index.php/XXI\_FSA/article/view/1274/, accessed 6/29/22, GDI- CC]

During the COVID-19 pandemic, the need for more security in the digital world has  heightened. Because of the increased online presence, requested to preserve human social and  professional relations, new opportunities emerged for cybercriminals who targeted the online  commerce and financial tools, as well as the healthcare system.

The EU High Representative Josep Borrell, in April and the NAC, on 3 June 2020,  condemned the destabilizing and malicious cyber activities performed in the context of the  coronavirus pandemic (Statement by the North Atlantic Council concerning malicious cyber activities  2020). NATO statement expressed the solidarity and mutual support for those affected by malicious  cyber activities, including healthcare services, hospitals and research institutes. The statement also  requested the respect for international law and norms of responsible state behavior in cyberspace  after disinformation campaigns conducted from China or Russia flooded Western media and social  networks.

The limited military cyberspace resources have to be employed carefully, only in the  necessary areas otherwise the Internet could easily absorb entire cyber capabilities. The military  activities have to remain limited in the cyberspace, targeting only specific areas of interests. The  largest part of cyber activities is performed and controlled by private entities in both EU and US, and  all allied operations and missions have some degree of reliance on civilian government or private  industry, mainly in the field of communications infrastructure, logistics, equipment, or host nation  critical national infrastructure.

Alexander Glenn, senior research for NATO and Cyber policy, identified four major  cyberspace activities related to the military: intelligence, information, crime and military operations:  “militaries participate in intelligence operations, conduct information operations, conduct and support  conventional and special operations, and respond to a limited subset of crime. Together these four  areas make up the military cyber domain (Crowther 2017).”

### Uniqueness – core function

#### NATO focus on core functions to develop integrated plan for Russia – strategic ambiguity good in this context

**Shea, 2022**

[Jamie, Associate Fellow, International Security Programme “NATO must now transform old missions into new strategy” Chatham House, June 21 2022 <https://www.chathamhouse.org/2022/06/nato-must-now-transform-old-missions-new-strategy> accessed GDI-TM]

A NATO strategic plan is now needed

The other issue for NATO is to develop a **single theatre-wide strategic plan** managed by the Supreme Allied Commander, Europe (SACEUR) and the NATO command structure. In reinforcing the alliance’s eastern flank, allies have sent forces to wherever they like and largely under national command, but this would not work in a real war.

NATO must revise its exercises to prepare and train for the new threat level, ensuring its forward deployed forces are fully integrated with local forces and the police and border guards to anticipate and respond to any Russian hybrid war tactics. It also needs to step up its joint planning and interoperability with Sweden and Finland and bring their territories into its standing defence plans.

One thing NATO has done well in this crisis is its political messaging. As Russia has become more threatening and reckless, it has been essential for NATO to be consistent and predictable. Re-affirming its core defensive purpose, calmly rejecting Putin’s nuclear posturing, and refusing to put NATO forces in Ukraine may be frustrating for some but it is vital not to play into Putin’s playbook regarding an ‘aggressive NATO’ or give him the sense he is being pushed into a corner. However, NATO strategic ambiguity can be useful when considering how to respond to a Russian escalation in Ukraine itself, such as using chemical weapons.

### NATO focus good - LIO

#### NATO refocus on core mission now – key to revitalizing the international order

**Shea, 2022**

[Jamie, Associate Fellow, International Security Programme “NATO must now transform old missions into new strategy” Chatham House, June 21 2022 <https://www.chathamhouse.org/2022/06/nato-must-now-transform-old-missions-new-strategy> accessed GDI-TM]

NATO is revived and refocused Although the Russian invasion of Ukraine is a catastrophe for Ukraine and Europe more generally, the multilateral system has discovered a new energy and sense of purpose as NATO has been revived and refocused on its core mission. The EU and the US have pulled together with daily coordination of their policies and actions, and the EU is also facing up to its geo-political role, as recognizing the EU aspirations of Ukraine, Moldova, and Georgia as well as the countries of the western Balkans shows its responsibility for the security and economic integration of the whole of Europe. The G7 has also taken on a more day-to-day operational role and the democracies of the Atlantic and the Pacific have united with only a few exceptions, such as Israel which is attempting to play a mediating role. The United Nations (UN) has also been reasonably robust with the General Assembly finding a new lease of life. Elsewhere, the World Health Organisation (WHO) is highlighting Russia’s destruction of hospitals, the Food and Agriculture Organisation (FAO) is stepping up to handle the fallout from reduced Ukrainian and Russian grain exports, the International Maritime Organisation (IMO) is intervening in the shipping crisis, and the International Criminal Court (ICC) is swinging into action to investigate and – hopefully – prosecute Russian war crimes. The narrative of a 21st century contest between the democracies and the authoritarians has been validated, even if it is too simple to explain all the complexities and nuances of the 21st century world. There is an opportunity for the transatlantic community to better defend itself and to build a more effective and values-based multilateral order able to react more systematically to rule-breaking and aggression – the question now is whether it will have the wisdom and skill to do so.

## Russia China Alliance

### China – Russia alliance – brink

#### China faces decision on international participation – alliance with Russia poses risks to China stability, creates opportunity for China to become participant in new international order

**Zelikow,** Professor of History at the University of Virginia and Executive Director of the 9/11 Commission, **2022**

[Philip, “The Hollow Order Rebuilding an International System That Works” Foreign Affairs July/August 2022 <https://www.foreignaffairs.com/articles/world/2022-06-21/hollow-order-international-system?utm_medium=social&utm_campaign=tw_daily_soc&utm_source=twitter_posts> accessed July 4 GDI-TM]

Yet a revised system of world order shouldn’t be limited to the United States and its traditional allies. It must be open to any countries that can and will help attain its common objectives. India should have a place at any symbolic high table, for example, as a permanent member of the UN Security Council. But India’s leaders are still making their choices about their will and capacity to work on common problems. Even China should be welcome at the table. After much internal debate in the early 1990s, China’s leaders chose to play a major and often constructive role in the global commonwealth system that emerged after the end of the Cold War. In 2005, Zoellick famously urged Beijing to become a “responsible stakeholder.” As late as 2017, Kurt Campbell, who now leads Asia policy for the Biden White House, thought this invitation was a wise move.

But Zoellick’s words were a challenge, one that Beijing is failing to meet. China’s partnership with Putin—whom Xi described to the Russian press as “my best and bosom friend”—is the opposite of responsible. Instead, it shows that China and Russia lead a primarily Eurasian grouping of dangerous states, including the likes of Iran, North Korea, and Pakistan. Their loose confederation has its cross-purposes and is united mainly by hostility toward the United States. But it is building tighter links, better divisions of labor, and more effective coordination than existed among the Axis powers before or during World War II.

For these and other reasons, pessimists believe China is irredeemably hostile. They argue that China has written off the United States as a country determined to resist China’s rise and that Chinese leaders may feel they have little to lose by embracing confrontation. In this pessimistic view, China is trying to shift from the post–Cold War era’s emphasis on global interdependence toward a Chinese grand strategy of Eurasian dominance and growing national self-sufficiency. China’s leaders are now using the pandemic to keep a chokehold on international travel and strengthen domestic surveillance.

That does seem to be China’s current plan. But it is unclear whether this plan will work. It rests on unproven social, political, and economic premises that are starting to deeply disturb parts of Chinese society essential to its past and future success—such as the many residents of Shanghai who have been trapped during the city’s draconian recent lockdown.

Chinese leaders may also have noticed that, in backing the Putin regime, they have tethered themselves to an adventurist Russian government that, for 30 years, has treated its neighbors much as Japan treated China between 1915 and 1945. For instance, Putin insists that Russia is not invading Ukraine. There is no war, he declared; there is only a “special military operation.” Many Chinese people will recall that, from 1937 to 1941, Japan insisted that it, too, was not invading China. There was no war, the Japanese said; there was merely a “China incident.”

Throughout the years of Japanese aggression, the United States defended China’s territorial integrity. Even amid times of misjudgment and weakness, Washington maintained that stance, refusing in November 1941 to make a deal with Japan at China’s expense. Ten days later, Japan went to war against the United States. As they watch what is happening in 2022, Chinese leaders can still reflect on this past and consider what decisions to make.

If Beijing charts a new course, it would not be the first time it has chosen to change. But if China does rejoin a system of world order, it should be a new one. The old system has fractured and must be remade. Facing tragic realities, the citizens of the free world must rebuild a global order that is practical enough to address the most vital common problems, even if it cannot and does not promise progress on all the values and concerns people face. This system will be far more effective if the world’s most populous country joins it, and China faces another time of choosing. Regardless of China’s participation, responsible actors must begin the hard, substantive work of protecting the planet from war, climate, economic, and health risks. The time for rhetoric and posturing is over.

## 