CEPA

Center *for*
European Policy
Analysis

May 2016


# Moving Toward NATO Deterrence for the Cyber Domain

## Cyber Intelligence Brief No. 1

Patrik Maldre

www.cepa.org

**Patrik Maldre** is an Adjunct Fellow at the Center for European Policy Analysis (CEPA), where he leads the CEPA Cyber Defense Initiative. Mr. Maldre is the author of numerous publications on cyber security threats and international cyber cooperation in the Baltic Sea region. His current research interests revolve around transatlantic cyber security policy, including cyber deterrence, norms, and confidence-building measures, as well as the use of offensive cyber capabilities during conflict and peacetime by threat actors connected to Russian strategic interests. Over the years, Mr. Maldre has worked with industry leaders and news organizations to identify and assess the use of Russian cyber capabilities and put them in strategic context for the public and transatlantic policymakers.

CEPA
Center *for*
European Policy
Analysis

# Table of Contents



CEPA

Center *for*
European Policy
Analysis

# THE ISSUE

**The run-up to the 2016 NATO Summit in Warsaw and the coming U.S. presidential election have brought NATO's future into sharp focus on both sides of the Atlantic. Detractors claim the alliance is a Cold War relic, and that it does not and cannot rise to meet the multi-dimensional security challenges of the 21st century. Nevertheless, NATO's 28 member states still affirm its strategic utility and invest in its capabilities. In the coming months and years, NATO must continue to modernize and adapt in response to rising threats. This is especially the case with cyber defense, which will play an increasingly pivotal role in the alliance's postures and plans. It is time to start moving toward NATO deterrence for the cyber domain.**

**Collective defense and deterrence have been foundational pillars of NATO strategy since the alliance's inception. Today, worsening tensions with Russia have once again pushed conventional deterrence to the top of the summit agenda. Unlike the Soviet Union, however, Russia possesses and employs advanced offensive cyber capabilities. NATO has agreed that strategic cyber attacks are subject to collective defense responses. These considerations—along with the digitization of NATO countries' modern military and civilian infrastructure—demand that conventional deterrence efforts be complemented by measures to discourage aggressive computer network operations. To do this, NATO and its member states must move beyond complacency and mistrust in their cyber defense frameworks. The alliance needs to be better able to not only deny benefits to adversaries operating in the cyber domain but also collectively punish—in accordance with international law—anyone who tries to cause large-scale disruption or destruction through offensive cyber capabilities.**

# NATO's digital journey

Cyber deterrence is still the subject of much skepticism, if not controversy, at NATO's Brussels headquarters and in the capitals of member countries. NATO's traditional mandate and priority has always been protecting its own communication networks. In fact, NATO technical agencies were safeguarding the confidentiality, integrity and availability of data at rest and in transit long before the word "cyber" entered into the official lexicon or ever appeared in the text of political agreements. That first happened in NATO's 2002 Summit in Prague and received further articulation at the 2006 Summit in Riga. It has been on the agenda ever since—its importance flowing and ebbing according to the strategic context and political will of national leaders.

Perhaps the single biggest external shock to NATO members and their views of digital security happened in 2007 in Estonia amid tensions between that country and Russia over the relocation of a Soviet war memorial in Tallinn. During a four-week period in late April and early May of that year, government, media and industry websites came under sustained distributed denial-of-service (DDoS) and defacement attacks.[1] Similar tactics took place during Russia's 2008 invasion of Georgia.[2] This prompted NATO members to pay more attention to the role computer network operations can play during political and military crises. Capitalizing on this momentum, NATO in 2008 adopted its first Policy on Cyber Defense and created the NATO Cooperative Cyber Defence Centre of Excellence (CCDCOE) in Tallinn.[3]

The last major leap forward for NATO cyber defense took place at the 2014 NATO Summit in Newport, Wales. On that occasion, member states formally signed the Enhanced Cyber Defence Policy and its accompanying action plan, which, among other things, affirmed the applicability of international law in cyberspace and confirmed that cyber attacks would be subject to collective defense responses. The Wales Summit also formalized the Estonian Defence Forces cyber range as the basis for NATO's cyber range capability. This was a significant development for NATO in the areas of capacity building, training, education and exercises. It also foreshadows a direction in which the alliance could head; namely, making national capabilities available to other member states. Finally, the summit also launched the NATO-Industry Cyber Partnership in order to strengthen NATO's relations with the private sector—a partnership member states called "crucial to enable NATO and Allies to achieve the Enhanced Cyber Defence Policy's objectives."[4]

> **"It is time to start moving toward *NATO deterrence for the cyber domain.*"**

# State of play

The streamlining of NATO's cyber defense governance structure was one of the primary accomplishments of NATO's most recent policy. As it stands, NATO's highest political authority naturally rests with the North Atlantic Council (NAC). As with other collective defense responses, that body would also make decisions in case of cyber attacks that threaten Euro-Atlantic security. The Cyber Defence Committee (CDC), in turn, provides daily political oversight and advice to member states. Likewise, the Cyber Defence Management Board (CDMB)—whose members are the heads of the political, military and technical agencies with information security roles—handles working-level topics. The NATO Communications and Information Agency (NCIA) is responsible for acquisition and implementation of NATO's cyber defense capabilities.[5]

The NATO Computer Incident Response Capability (NCIRC), part of the NCIA, is the day-to-day shield that protects NATO from cyber attacks. The unit achieved full operational capability in 2013 and provides centralized, around-the-clock information security services to 41 military and civilian installations on both sides of the Atlantic. According to the NATO Secretary-General's annual report, "NATO responds to millions of suspicious cyber events on a daily basis, the majority of which are detected and mitigated automatically."[6] Of these, an average of 320 incidents per month NATO-wide in 2015 were considered serious enough to require manual responses, a 20 percent increase over 2014. NCIRC is at the forefront of NATO's technical resilience, "providing specialist services to prevent, detect, respond to and recover from cyber security incidents."[7]


North Atlantic Council visits NATO Cyber Security Centre - NATO Multimedia Library/NIDS.

NATO's information security in a broader sense, however, relies largely on member states, with national agencies protecting the infrastructure used to process data and communications between allied capitals and NATO sites. Furthermore, NATO's collective conventional capabilities, operations and plans could be exposed by breaches of member-state ministries and parliaments. For this reason, NATO has signed a memorandum of understanding with all member states to improve information sharing and situational awareness.[8] It has also signed a similar accord with the European Union.[9] Furthermore, NATO has also created a Rapid Reaction Team (RRT) to assist member states in case of national crises that threaten NATO security.[10] Finally, NATO and member states organize annual technical and operational-level cyber defense exercises based in Estonia, cooperate on several different Smart Defence initiatives related to information security, and implement high-level research projects and working groups focused on cyber defense.[11] Clearly, NATO is acting on a variety of defensive fronts. This is necessary, but not sufficient.

**"Clearly, NATO is acting on a variety of defensive fronts. *This is necessary, but not sufficient.*"**


Bill Roche/U.S. Army Cyber.

# The Russian cyber threat

NATO and its member states face network intrusion attempts and denial-of-service attacks from a wide spectrum of adversaries. This list includes hacktivists, cybercriminals, terrorists, state-sponsored groups and rival military and intelligence agencies. In the cyber domain, it can be quite difficult to distinguish among them. However, some threats can be identified and prioritized over others. Several allies place Russia at the top of the list. Estonia's foreign intelligence agency recently asserted that "in cyberspace, Russia is the source of the greatest threat to Estonia, the European Union and NATO."[12] The U.S. Office of the Director of National Intelligence's worldwide threat assessment for 2016 put "cyber and technology" as one of the nation's top security threats, with Russia as the leading threat actor.[13] Recent operations against Turkey's leadership[14], Germany's parliament[15] and a French media company[16] indicate that advanced Russian cyber operations are a NATO-wide threat that must elicit a NATO-wide response.

Tensions between NATO and Russia are at their worst since the end of the Cold War, mainly because of Russia's 2014 invasion of Ukraine. But cyber threat actors with connections to Russia were conducting offensive computer operations long before Russia annexed Crimea and occupied eastern Ukraine. Many sophisticated malware platforms used by Russian threat actors (Dukes, Snake, APT28) date back to 2007 or even earlier.[17] They have been conducting campaigns against virtually every country in the alliance. Cyber capabilities are now fully integrated into Russia's overall foreign and security policy toolbox. These actors, furthermore, are growing increasingly bold and unpredictable in their activities, especially those that target critical infrastructure. Some groups, such as Energetic Bear, have the capacity for "sabotage" but appear not to have employed it.[18] On the other hand, a December 2015 attack against Ukraine's electric grid left a quarter of a million people in the dark.[19] The trend is toward the development and use of capabilities intended not only to steal information but also to manipulate systems and data in order to cause physical and economic damage. That could not only undermine NATO unity but more broadly damage strategic stability.

Consider one potential scenario. Tensions continue to rise between Russia and NATO, as allies continue to protest against incidents at sea, border violations, and airspace incursions. During a 2017 NATO Foreign Ministerial, a coordinated cyber operation suddenly hits a member state, crippling multiple critical infrastructure sectors, such as railways, electric grids and mining operations. At the same time, DDoS attacks overwhelm many of the country's media and government websites, while others are breached and defaced. Citizens and businesses are left in the dark while incident responders struggle to analyze the situation. Domestic and international rail travel grinds to a halt. The mining industry suffers serious economic losses. The country's own computer emergency response teams are overwhelmed by organizations needing help to restore functionality, and its government realizes that it faces a national security emergency. Yet does this constitute a cyber attack that should trigger a collective defense response by NATO? The North Atlantic Council—the highest body responsible for determining NATO's response—is already meeting at the ministerial level. Members disagree whether they should interrupt their regular schedule to discuss the emerging crisis. Press coverage abounds. Desperate, the country invokes Article 4 and NAC decides to deploy the Rapid Reaction Team. The RRT detects well-known Russian malware samples in affected networks and traces substantial portions of incoming DDoS traffic to Russian servers, among a variety of other technical and political indicators. The first casualties occur as trains collide. Mining companies declare losses reaching into the millions. Some regions still lack access to electricity. The country blames Russia and invokes Article 5. What will NATO and its member states do?

As this scenario and others practiced during Locked Shields, Cyber Coalition and other exercises make clear, NATO must be ready to confront large-scale cyber operations conducted by unfriendly, well-resourced actors. First, member states must come to some form of agreement about what constitutes a cyber attack requiring a collective defense response. The outward policy of "strategic ambiguity"—or leaving it up to a political decision by the NAC if it happens—may keep adversaries guessing. But internally, NATO cannot afford to wait until a crisis before it makes a decision. It needs some defining criteria ahead of time, even if only at the classified level. Better yet, NATO can and should continue to make technological advancements and take political measures to prevent potential adversaries from conducting such attacks in the first place. Rather than simply developing defensive measures, NATO and its member states need comprehensive—and preferably public—strategies that impose costs on Russia and other adversaries which currently lack incentives to do otherwise. They operate with impunity, plausible deniability and increasing boldness. In an atmosphere of increasing tensions, the current state of affairs may lead to miscalculation and unnecessary escalation. The move toward a bold new strategic framework of deterrence can help avert both while discouraging Russia's aggressive behavior in the cyber domain.


Locked Shields 2016 cyber defense exercise - Hans-Toomas Saarest/Estonian Defence Forces.

# The long road to deterrence

Cyber deterrence clearly warrants more discussion among NATO members than ever, given the threats they now face—particularly from the East. Yet the Cyber Defence Committee doesn't really cover it, nor will a full-fledged cyber deterrence concept be announced at the upcoming NATO summit in Warsaw. The main debate in Brussels and in national capitals centers on whether cyberspace should even be considered a domain of warfare, as many member states have already decide; the fuzzy concept of active cyber defense is only tentatively mentioned. However, senior NATO leaders have espoused deterrence as a potential future direction for the alliance. Importantly, several member states, including the United States, Britain and Estonia, are also publicly exploring such a strategy.[20] The moment is not yet right for an alliance-wide declaration on this topic, but with concerted effort at all levels, NATO can and should continue to move toward deterrence for the cyber domain.

Deterrence aims to discourage an adversary from taking offensive action. Traditionally, its two pillars have been deterrence-by-denial and deterrence-by-punishment. The first refers to measures that reduce or eliminate the benefits of a certain aggressive move, while the second seeks to impose additional costs for performing it. NATO's traditional mandate of defending its own systems fits comfortably into the deterrence-by-denial part of this framework. Deterrence-by-punishment, however, is far more controversial because of the problem of attribution—which refers to the difficulty of identifying the perpetrators of operations. Finally, both concepts also rely on intent, capability and credibility. As it stands, a palpable lack of trust among member states hinders collective action on both fronts. Progress in the denial category will be easier and more visible, but countermeasures should be considered as well.

NATO has come a long way in terms of working together to shore up technical defenses in cyberspace. The main barrier to further cooperation, however, is the difference in technical and administrative capacities as well as human and financial resources among member states. This, along with differing national views, remains the main barrier to further integration. The alliance is only as strong as its weakest member. When it comes to deterrence-by-denial, therefore, all member states must have the basics in place: computer security laws, national cyber strategies, a police focus on cybercrime, national CERTs, public-private partnerships and capable intelligence agencies. From there, members should enact effective, actionable information-sharing programs. After that, the next step is to develop joint situational awareness. Typically, adversary espionage campaigns target multiple NATO and member-state organizations simultaneously. Early warning and shared situational awareness can prevent multiple entities in different countries from being breached by the same operation. The end goal for the denial part of the deterrence strategy is, of course, resilience. If NATO and its members can effectively work together to prevent, detect, respond and recover from cyber attacks, this would significantly decrease the benefits and increase the costs for an adversary. NATO collective action should continue in this direction, and joint efforts can help to promote trust and confidence—a key ingredient in further cooperation in deterrence-by-denial, but even more crucial when it comes to deterrence-by-punishment.

Preventing adversaries from benefitting from offensive actions, or at least limiting their gains, can help discourage them from conducting such attacks in the first place. Punishing them after the fact is another. While the term has an aggressive connotation, this part of the strategy is defensive and retaliatory in nature. It can refer to a broad spectrum of actions—from naming-and-shaming to nuclear strikes. In the cyber domain, the problem of attribution hinders the goal of effective deterrence. For this reason, NATO and its member states should invest heavily in the technological and analytical capabilities necessary to discern signs of a particular adversary, including in cooperation with the private sector.

As numerous cases of attribution to Russian cyber threat actors demonstrate, this is already taking place. Furthermore, member states should complement technical attribution with political and diplomatic attribution. Currently, months and even years pass before politicians and leaders feel comfortable about ascribing blame. For deterrence to work, however, governments must carry out both high-level and private attribution in conjunction with media and private companies as soon as they have conclusive evidence. Calling out threat actors and their state sponsors in diplomatic forums, public discussions and private meetings can motivate them to conduct less aggressive operations.

NATO and its member states should also adopt joint approaches to developing and employing offensive capabilities for collective defense purposes. Laudably, many individual allies have already declared that they possess such capabilities and the doctrines for using them. However, considerable mistrust persists among the allies, creating an atmosphere of uncertainty and doubt—which weakens deterrence as a whole. To overcome this hurdle, allies can begin by making political statements about potentially using these capabilities in case of attack, and in accordance with international law as part of a collective defense response. Ultimately, NATO should move toward sharing these capabilities, perhaps by using existing models based on nuclear doctrine. Transparency and straightforwardness in this arena could contribute substantively to deterring adversaries and reinforce collective defense among NATO members.

Intent and credibility will play into adversaries' calculations for any type of countermeasure. For this reason, policy innovations and capability development need to be complemented by effective strategic communication. You cannot achieve deterrence if your adversary doubts that you'll do what you say—and even less so if it doesn't think you can do what you say. From this perspective, demonstrations such as the Aurora test in 2007 can be quite useful.[21] Other, more subtle means include presentations by top officials at security conferences. Operations against third-party adversaries other than the intended target of deterrence can also deter attacks; few doubt that Russia paid close attention to the Stuxnet case, or that NATO drew conclusions from the Ukraine grid attack. In sum, effective strategic communication—both public and private—can be a key component or complement of a deterrence-by-punishment strategy.

Finally, deterrence should be seen as a cross-domain strategy. Individual allies that are crafting and in some cases already implementing their deterrence strategies have rightfully begun to employ the full set of national power toward achieving this objective. This can and should include law enforcement tools, judicial means and economic options; in extreme cases, such a strategy should also incorporate military strikes. The first three are largely outside of the purview of NATO as an international organization. However, the last certainly falls within its mandate. If a cyber operation is attributed to Russia or any other actor and the NAC decides that it amounts to an act of war requiring a collective defense response, NATO should keep the military option on the table as a matter of doctrine. Once again, individual allies have already made such declarations; NATO as a political and military alliance can and should do the same.

# Conclusion

NATO is a pillar of transatlantic security and stability. However, it faces challenges internally from those who doubt its relevance to the 21st century, as well as externally, from a resurgent and aggressive Russia. If NATO's member states want to ensure that the alliance continues to rise to the occasion, they must remain committed to the ever more important question of cyber defense. Today's NATO faces a different kind of Russia—one that does not hesitate to conduct offensive operations against the alliance in the digital terrain. NATO should not only internalize the fact that cyberspace has become a domain of warfare; it should also start adopting strategies to enhance collective defense and security in this new era. The strategy of deterrence provides a framework that NATO can use in the long term to address cyber threats, just as it uses it in conventional defense and nuclear policy. In fact, such a strategy will be most effective if members integrated it into the overall alliance posture. In this way, NATO can keep adjusting to emerging threats and bring allies closer together—not only in questions of security and defense, but upon the foundation of values they all share and promote.

**"You cannot achieve deterrence if your adversary doubts that you'll do what you say—*and even less so if it doesn't think you can do what you say.*"**

Cyber Shield 2016 - Sgt. Stephanie A. Hargett/U.S. Army Cyber.

# Endnotes

1. Traynor, Ian, “Russia accused of unleashing cyberwar to disable Estonia,” *The Guardian,* May 2007.

2. Markoff, John, “Before the gunfire, cyberattacks,” *New York Times,* August 2008.

3. Kaiser, Ryan P., “Estonia: NATO’s Cyber Warrior,” Center for European Policy Analysis, May 2008.

4. Wales Summit Declaration,” NATO, September 2014.

5. “Governance: Cyber defence,” NATO, February 2016.

6. Stoltenberg, Jens, “The Secretary General’s Annual Report: 2015,” NATO, January 2016.

7. “Cyber Security,” NATO Communications and Information Agency, 2014.

8. Stoltenberg, Jens, “The Secretary General’s Annual Report: 2015,” NATO, January 2016.

9. “NATO and the European Union enhance cyber defence cooperation,” NATO Communications and Information Agency, February 2016.

10. “Men in black – NATO’s cybermen,” North Atlantic Treaty Organization, April 2015.

11. Stoltenberg, Jens, “The Secretary General’s Annual Report: 2015,” NATO, January 2016.

12. “International Security and Estonia: 2016,” Estonian Information Board, March 2016.

13. Clapper, James R., “Statement for the Record: Worldwide Threat Assessment of the US Intelligence Community,” Senate Armed Services Committee, February 2016.

14. Hacquebord, Feike, “Pawn Storm Campaign Adds Turkey To Its List of Targets,” Trend Micro, March 2016.

15. “Russia ‚was behind German parliament hack’,” BBC News, May 2016.

16. Hardy, Catherine, “Russian hackers blamed for TV5 cyber attack,” Euronews, June 2015.

17. Maldre, Patrik, “Global Connections, Regional Implications: An Overview of the Baltic Cyber Threat Landscape,” International Centre for Defence and Security and Baltic Assembly, September 2015.

18. Finkle, Jim, “U.S. government asks firms to check networks after ‚Energetic Bear’ attacks,” Reuters, July 2014.

19. Zetter, Kim, “Inside the cunning, unprecedented attack hack of Ukraine’s power grid,” *Wired,* March 2016.

20. Maldre, Patrik, “Wanted: Cyber Deterrence,” Center for European Policy Analysis, March 2016.

21. Meserve, Jeanne, “Sources: Staged cyber attack reveals vulnerability in power grid,” CNN Breaking News, September 2007.


Center *for*
European Policy
Analysis


Center *for*
European Policy
Analysis

Cover photo - U.S. Army photo by Mike Strasser/USMA PAO

The Center for European Policy Analysis (CEPA) is the only U.S. think-tank dedicated to the study of Central and Eastern Europe. With offices in Washington and Warsaw, it has grown rapidly over the last decade to become the leading voice for strengthening security and democracy in the countries of post-Communist Europe. CEPA is at the forefront of the transatlantic policy debate on issues of defense, energy and democratic reform in Central and Eastern Europe. Its mission is to promote an economically vibrant, geopolitically stable and politically free Central and Eastern European region with close and enduring ties to the United States.



Center for European Policy Analysis
1225 19th Street NW, Suite 450
Washington, DC 20036
E-mail: info@cepa.org
www.cepa.org


Center *for*
European Policy
Analysis