Hudson Institute

Strengthening NATO Cyber Defense Under U.S. Leadership

Ambassador Sorin Ducaru, Ph.D.
Senior Fellow

April 2018
Briefing Paper

Hudson Institute

Strengthening NATO Cyber Defense Under U.S. Leadership

Ambassador Sorin Ducaru, Ph.D.
Senior Fellow

For more information about obtaining additional copies of this or other Hudson Institute publications, please visit Hudson's website, www.hudson.org

ABOUT HUDSON INSTITUTE

Hudson Institute is a research organization promoting American leadership and global engagement for a secure, free, and prosperous future.

Founded in 1961 by strategist Herman Kahn, Hudson Institute challenges conventional thinking and helps manage strategic transitions to the future through interdisciplinary studies in defense, international relations, economics, health care, technology, culture, and law.

Hudson seeks to guide public policy makers and global leaders in government and business through a vigorous program of publications, conferences, policy briefings and recommendations.

Visit **www.hudson.org** for more information.

Hudson Institute
1201 Pennsylvania Avenue, N.W.
Suite 400
Washington, D.C. 20004

P: 202.974.2400
info@hudson.org
www.hudson.org

Table of Contents

Summary

This paper defines a framework for a coherent NATO cyber strategy, led by the U.S., which would build on the transatlantic alliance to forge a stronger platform for cyber cooperation and cyber defense.

Washington has taken the lead in promoting several important NATO initiatives, such as defining effective nuclear and counterterrorism strategies and establishing the Enhanced Forward Presence at the eastern frontier of the alliance. However, American leadership has been less focused and robust in promoting the alliance's cyber agenda. The United Kingdom and other European allies championed important developments first. These included linking cyber to NATO's core task of collective defense and recognizing cyber as a domain of military operations. Decisive U.S. support came only later in the process.

Today, unprecedented state-sponsored cyberattacks are targeting critical infrastructure and democratic institutions. Their increasing use in crisis environments and hybrid warfare highlights the need for NATO to do much more to bolster its cyber-defense capabilities as follows:

1. Define cyber defense as a top strategic priority for NATO members.
2. Promote a comprehensive, cross-domain strategy to deter cyberattacks.
3. Accelerate implementation of the cyber operational-domain roadmap.
4. Improve situational awareness within NATO by creating a joint cyber situational-awareness and attribution platform.
5. Develop cyber capabilities faster, including creating a more flexible procurement process for IT.
6. Make better use of NATO as a political platform. In cyber-related crisis situations, utilize NATO for consultation, strategic communications, decisions on joint response, and collective defense and deterrence.
7. Use NATO's institutional assets to address the tremendous need for skills and talent in cyber defense.
8. Support stronger cyber partnerships with trusted non-NATO partners.

As with past NATO challenges, robust U.S. leadership and cooperation with allies will be indispensable to timely and successful implementation of these key priorities.

I. Background: The Evolution of NATO Cyber Defense

Over the past several years, cyberattacks have dominated headlines across the world. While this may seem like a relatively new phenomenon, NATO's encounters with cyberattacks began decades ago. In the late 1990s, during NATO's involvement in ending the conflict in Kosovo, its communication networks sustained multiple attacks. At that time, the cyber issue was regarded largely as a technical issue that could be solved primarily through technical means, rather than a topic of growing strategic concern.

2008: NATO Establishes a Cyber-Defense Policy

In April 2008, one year after major cyberattacks against NATO member Estonia, the alliance developed its foundational cyber-defense policy, which placed cyber issues on NATO's political agenda for the first time. The policy's focus was the cyber resilience of NATO's own networks.

The policy established a division for cyber responsibilities and a cyber-defense-management structure within NATO, the Cyber Defence Management Board (CDMB). It also created mandatory cybersecurity benchmarks and requirements, including more secure systems architecture to protect NATO networks and guidelines for allied national networks. While NATO's main responsibility was to protect the organization's networks, each member country was held responsible for its own national networks. One important resource established in 2008 was NATO's Cooperative Cyber Defence Centre of Excellence in Tallinn, Estonia.

2011: NATO's Cyber-Defense Policy Gets an Upgrade

In November 2010, NATO adopted the Lisbon Strategic Concept, which emphasized the need to more thoroughly address fast-evolving twenty-first-century security challenges, including cyberattacks. NATO then updated its cyber policy in June 2011, adopting a centralized approach to protecting its networks across more than 50 sites, including its civilian headquarters (Military Command Structure) and specialized agencies.

The new policy extended its focus beyond protecting NATO's own networks and towards establishing agreed-upon benchmarks to protect the allies' national networks. These benchmarks have been defined as "cyber-defense-capability targets" to be met by each ally within the NATO Defence Planning Process (NDPP). They include requirements for national cyber strategies as well as policies, training, education, exercises, information-exchange platforms, and computer-incident response teams. The policy also provided mechanisms for allied nations to exchange cyber information and conduct cyber-threat analysis through training, education, and exercises.

Major practical achievements stemming from this new policy included NATO's Malware Information Sharing Platform (MISP) and Cyber Threat Assessment Cell (CTAC), the establishment of NATO's cyber rapid-reaction teams, and the launch of annual NATO Cyber Coalition exercises.

2014: Wales Summit: "Enhanced NATO Policy on Cyber Defense"

The steps taken in 2011 paved the way for a cyber inflection point in 2014. At that year's NATO summit in Wales, the allies adopted a third cyber-policy document, which made the cyber domain one of their key political and strategic priorities. This was reflected in three of the policy's central elements: linking cyber to the core alliance task of collective defense, recognizing that international law applies in cyberspace, and engaging non-NATO nations for potential cyber partnerships**.**

2016 Warsaw Summit: Recognizing Cyberspace as a Domain of Military Operations

At the Warsaw Summit in July 2016, the allies recognized cyberspace as a new "operational domain in which NATO must defend itself as effectively as it does in the air, on land and at sea." Cyberspace was implicitly acknowledged as a "digital battleground" that requires strategic attention and new approaches to operational planning, training, and resourcing. Most importantly, this was guided by the realistic assumption that future NATO operations and missions will operate in a highly contested cyber environment where the enemy will attack, and potentially degrade, NATO cyber capabilities.

NATO's recognition of cyberspace as a military domain paved the way for it to integrate its cyber efforts into operations and missions through offensive cyber capabilities. However, the allies decided that NATO as an organization would not develop, acquire, or employ any offensive cyber capabilities. Instead, as in the other operational domains, NATO would rely on the broad range of member nation capabilities.

In November 2017, the allies adopted a set of principles for incorporating voluntary national contributions of offensive cyber capabilities into NATO's operational planning. These principles included political oversight and legal guidelines. The core of this framework is the agreement that in cyberspace, as in other operational domains, NATO will act in accordance with its defensive mandate and with international law. In February 2018, the allies set up a Cyber Operations Centre within NATO's Military Command Structure.

II. Limitations of NATO's Current Cyber Policy

Despite real progress in NATO's approach to cyber issues, significant limitations and weaknesses in its current cyber posture remain:

- There is still no comprehensive strategic doctrine aimed at deterring state-sponsored cyberattacks.
- The cyber posture lacks agility and seamless situational awareness. NATO also needs a renewed commitment to increasing the exchange of cyber information and intelligence and defining benchmarks for "information exchange interoperability."
- NATO lacks a common framework and standards for allies to assess their cyber vulnerabilities.
- IT procurement processes are slow and cumbersome.
- There is limited employment of cyberanalytics.
- There is no strategy to employ artificial intelligence to strengthen cyber defense.
- NATO has only two highly trained cyber rapid-reaction teams with state-of-the-art capabilities for cyber mitigation, analysis, and forensics. Under the current policy, they can be deployed only with the unanimous agreement of the NATO Council, a cumbersome process that is ill-suited to countering the speed of cyberattacks.
- The allies have yet to agree on how to integrate voluntary national contributions of offensive cyber capabilities into NATO operations and missions.
- NATO is insufficiently leveraged as a political platform for cyber-strategy consultation, cyber deterrence, and cyber-relevant strategic communications.

III. Policy Recommendations to Strengthen NATO Cyber Defense

1. **Define cyber defense as a top strategic priority for NATO members.** Such a decision is key to sustaining strategic-level attention to cyber issues among NATO's political leaders. It would also help secure a commitment for more substantive, coherent, and coordinated resourcing for cyber defense among allies. Currently, strategic-level attention to cyber issues is episodic, which limits resources allocated for cyber defense.

2. **Promote a comprehensive, cross-domain strategy to deter cyberattacks.** Cross-domain deterrence means that an aggressor calculating whether to launch a cyberattack against one or more NATO members will understand that an attack could be met with a broad spectrum of retaliatory actions. These might include a combination of political, economic, financial, cyber, and/or military responses. This range of potential responses offers the advantages of flexibility, diversity, visibility (compensating for the limited transparency inherent in cyber responses), proportionality (if desired), and scalability (the potential to control escalation, or to de-escalate). Public promotion of this deterrence strategy should reinforce the message that NATO has the same resolve to defend against cyberattacks that it has in other areas of collective security.

3. **Accelerate implementation of the cyber operational-domain roadmap.** After NATO's decision to recognize cyberspace as an operational domain, it adopted a 36-month implementation roadmap. This timeline needs to be accelerated under the leadership of the U.S. and other allies with advanced cyber capabilities.

   At the NATO defense ministers' meeting in February 2018, the allies agreed to form a Cyber Operations Centre within the NATO Command Structure. One important aspect of this "operationalization of cyberspace" within NATO is that member nations will voluntarily provide and integrate select offensive cyber capabilities for NATO's operations and missions, just as they provide conventional capabilities. The framework of political and legal principles for integrating such voluntary national cyber contributions was agreed upon at the end of 2017, and the UK has announced its readiness to volunteer relevant cyber capabilities to benefit the NATO alliance. U.S. leadership remains key to developing the doctrine, political oversight process, delegation of authority, rules of engagement, and military planning mechanisms to integrate cyber efforts within NATO.

4. **Improve cyber situational awareness within NATO and create a joint situational-awareness and attribution platform.** NATO has successfully invested in many platforms to increase its cyber situational awareness, such as the NATO Computer Incidents Response Centre (NCIRC), MISP, CTAC, and the cyber task force within NATO's Intelligence Division. Further consolidation of these resources and additional investment are needed to create a genuine joint cyber situational-awareness/attribution platform.

   Beyond the need for a consolidated situational-awareness platform and modernized capabilities, the allies need to make a fresh commitment to greater and faster sharing of relevant cyber information. Additionally, they should adopt an agreed-upon framework establishing benchmarks to ensure that these platforms have information interoperability and that there are procedures that safeguard use of this information.

5. **Develop cyber capabilities faster.**

    - **Change the procurement process for IT and cyber-defense capabilities within NATO.** The current process takes approximately five years and does not distinguish between the procurement of conventional defense platforms, which can have a relatively long service life, and IT systems, which need to be updated regularly in a rapidly changing threat environment.

    - **Create a platform for fast NATO access to cyber-defense innovation—for example, a cyber-defense incubator or an innovation exchange.** The allies should create a dedicated cyber innovation fund to foster innovation tailored to NATO's evolving cybersecurity needs. The NATO Communications and Information Agency (NCIA) in Brussels, and its Atlantic Command Transformation (ACT) in Norfolk, Virginia, could be locations for "incubators" where engineers and other personnel could draw from this fund to quickly develop tailored solutions to ensure dynamic protection of NATO's networks.

    - **Establish a uniform system of benchmarks and mechanisms for member states to self-audit their cyber vulnerabilities.**

    - **Increase the number of NATO cyber rapid-reaction teams, upgrade their expertise, and allow their rapid deployment to assist allies with cyberattacks.**

    - **Accelerate the introduction of cyber-analytics and artificial intelligence tools for cyber defense.**

6. **Increase NATO's leverage as a political platform in crisis situations sparked by cyberattacks.** NATO should regularly be used as a platform for high-level briefings, discussions, and possibly joint action by member nations in response to significant cyberattacks. One example would be a joint U.S.-UK initiative to brief the North Atlantic Council on the findings that led them to *publicly* blame the Russian military for the "NotPetya" attack. Such a briefing would clearly increase the number of allies that would associate themselves with this public attribution. Regular briefings on major cyberattacks would encourage more allies to publicly identify the source of the attack and increase the likelihood of a swift NATO-wide response.

    Additionally, NATO could trigger consultations under Article 4 of the Washington Treaty, which would signal allied solidarity and potentially prompt concrete actions. NATO could also invoke the collective defense clause of Article 5 should a cyberattack have consequences comparable to those of an armed attack.

    There is also a need to update NATO crisis response procedures to make them more relevant and effective in countering cyberattacks. Current NATO procedures are focused on several consecutive, time-sensitive “operational steps” to be taken in response to physical crises, and they emphasize movements of troops and military equipment and associated operational actions. For crises generated by cyberattacks, these time-consuming operational steps, tailored to respond to conventional attacks, should be replaced by much faster and more agile response procedures.

7. **Use NATO as a platform to address the tremendous need for talent in cyber defense.** NATO has developed several educational platforms. Two of the newest ones, the Cooperative Cyber Defence Center of Excellence in Tallinn and the NATO Communications and Information Systems School in Portugal, are dedicated to cyber-defense training. Legacy schools, such as the NATO Defense College in Rome or the NATO School in Oberammergau, Germany, could also be used to enhance the “digital IQ” of military leaders and policy makers. Furthermore, these schools could address the policy and operational implications of growing cyber threats and review relevant defense and deterrence strategies.

8. **Support stronger cyber partnerships with trusted non-NATO partners.** An ever-stronger NATO alliance in cyberspace should continue to develop its trusted cyber partnerships, as it is recognized that cyber defense is a team sport. NATO has developed cyber partnerships with trusted, like-minded nations such as Japan, South Korea, Israel, Sweden, and Finland. These partnerships need to be further developed, based on the mutual interests of NATO allies and partners, with a special focus on exchanging information and analysis on cyber issues, capability development, training, and exercises. This would increase allies’ and partners’ situational awareness, strengthen their cyber defenses, and support the aim of a more stable cyberspace.

Author Biography

Ambassador Sorin Ducaru, Ph.D.
Senior Fellow, Hudson Institute

Ambassador Sorin Ducaru recently served as the NATO Assistant Secretary General (ASG) for Emerging Security Challenges. He was responsible for providing support to the North Atlantic Council and for advising the Secretary General on the evolution of emerging security challenges. In this capacity, Ambassador Ducaru oversaw the implementation of NATO's enhanced cyber policy and chaired the NATO Cyber Defense Committee and Cyber Management Board. Prior to his appointment as ASG, Ambassador Ducaru served as the Permanent Representative of Romania to the United Nations between 2000-2001, Romania's Ambassador to the United States between 2001-2006, and as Romania's Permanent Representative to the North Atlantic Council from 2006-2013.

Ambassador Ducaru is currently anchoring a new cyber initiative at Hudson Institute that seeks to help transform the Atlantic Alliance into a stronger platform of cyber cooperation and cyber defense.

Hudson Institute is a research organization promoting American leadership and global engagement for a secure, free, and prosperous future.

Founded in 1961 by strategist Herman Kahn, Hudson Institute challenges conventional thinking and helps manage strategic transitions to the future through interdisciplinary studies in defense, international relations, economics, health care, technology, culture, and law.

Hudson seeks to guide public policy makers and global leaders in government and business through a vigorous program of publications, conferences, policy briefings and recommendations.

Hudson Institute
1201 Pennsylvania Avenue, N.W.
Suite 400
Washington, D.C. 20004

P: 202.974.2400
info@hudson.org
www.hudson.org