Atlantic Council
BRENT SCOWCROFT CENTER
ON INTERNATIONAL SECURITY

ISSUE BRIEF

Cyber, Extended Deterrence, and NATO

MAY 2016 FRANKLIN D. KRAMER, ROBERT J. BUTLER, AND CATHERINE LOTRIONTE

This paper sets forth a concept for cyber extended deterrence, focusing on a potential conflict involving NATO. The paper considers both deterrent and warfighting requirements including relevant doctrine and capabilities.

The paper recommends that NATO provide extended deterrence to help less cyber-capable nations defend their military, telecommunications, and electric grid infrastructures and to increase NATO's cyber capabilities as part of an integrated defense by:

- creating "cyber framework nations" each of which would lead a cyber framework group and support national capabilities including the establishment, transfer, training, and support of necessary cyber capabilities; the United States would be the first cyber framework nation;
- establishing operational partnerships, including at the national level, with key private entities, including ISPs and electrical grid operators; and
- developing doctrine and capabilities to provide for the effective use of cyber in a conflict as part of NATO's warfighting capabilities.

NATO could also consider recommending that the European Union create a "cyber reliability support initiative" that would fund upgrades to national infrastructure to enhance cyber resilience.

Introduction

Cyber is relevant in conflict as well as in lesser circumstances such as espionage and crime. This paper focuses on a conflict, both conventional and hybrid, with an adversary, such as Russia, that has advanced cyber capabilities (Tier V/VI as designated by the Defense Science Board)[1]

1 Defense Science Board, "Resilient Military Systems and the Advanced Cyber Threat," January 2013, pp. 2, 22, http://www.acq.osd.mil/dsb/reports/ResilientMilitarySystems.CyberThreat.pdf.

and includes a conflict with an improving, but less capable nation-state such as Iran. Extended deterrence, most often considered in the nuclear arena, involves a stronger ally providing a capability in support of allies that do not possess the capability and includes not only cost imposition, but also defense and resilience intended to reduce either the probability or the impact of an attack. The intention of providing such extended deterrence is that the Alliance as a whole will therefore be stronger from both geopolitical solidarity and capability standpoints.

Nature of threat

Over the last decade, there has been a continuing advancement of the cyber threat in both depth and breadth with the expansion of exploitation, disruption, and destruction activities. In an Internet-connected, net-centric world, military networks and key supporting critical infrastructures are now at significant risk from cyber intrusion. As Admiral Michael Rogers, head of Cyber Command, has testified,

> Digital tools in cyberspace give adversaries cheap and ready means of doing something that until recently only one or two states could afford to do: that is, to reach beyond the battlefield capabilities of the U.S. military. They have demonstrated the capacity to hold "at risk" our military and even civilian infrastructure. In lay terms, that means that decades of military investment is now imperiled, because as Secretary Carter says, our forces depend on the functioning of our military networks and combat systems, without which they, and we, are far less effective in all domains.[2]

What is true for the United States is equally, and even more, true for other NATO nations. The risks are widespread and substantial.

- The DoD Cyber Strategy itself states, "The Defense Department's own networks and systems are vulnerable to intrusions and attacks."[3] The Defense Science Board has reported that "cyber attack tools which can be downloaded from the Internet, are very successful at defeating our systems."[4] Admiral Rogers has testified that a "group of hackers was responsible for an intrusion into an unclassified network maintained by our Joint Staff."[5]
- Since 2007 and the Russian distributed denial-of-service (DDoS) attacks on the Estonian government and civilian entities, there has been a continued escalation of these types of attacks on nations in conflict situations, such as Georgia in 2008 and more recently Ukraine. Notably, NATO public websites and unclassified email were hit by DDoS attacks in March 2014, at the time of Russia's Crimea invasion.[6] In December 2015, Turkish government websites and financial institutions were targeted in a two-week long DDoS attack resulting in the disruption of services and transactions. In an effort to stop the attack, Turkey blocked all foreign internet traffic.[7] A European Parliament report has stated that cyber-attacks "have been directed to the military: grounding French naval planes, securing access to the UK Ministry of Defence's classified networks or attacking the Estonian Ministry of Defence (2013)."[8]
- Defense supporting industry is equally at risk. The Senate Armed Services Committee extensively analyzed intrusions into contractor networks supporting US Transportation Command, finding "approximately 50 successful intrusions" in a one

2 Admiral Michael S. Rogers, Commander, United States Cyber Command, "Statement before the Senate Committee on Armed Services," United States Senate Committee on Armed Services, September 29, 2015, http://www.armed-services.senate.gov/imo/media/doc/Rogers_09-29-15.pdf

3 Department of Defense, "The DOD Cyber Strategy (2015)," April 2015, p. 10, http://www.defense.gov/Portals/1/features/2015/0415_cyber-strategy/Final_2015_DoD_CYBER_STRATEGY_for_web.pdf

4 Defense Science Board, "Resilient Military Systems and the Advanced Cyber Threat (2013)," January 2013, p. 1, http://www.acq.osd.mil/dsb/reports/ResilientMilitarySystems.CyberThreat.pdf.

5 Admiral Michael S. Rogers, "Statement before the Subcommittee on Emerging Threats and Capabilities," House Armed Services Committee, March 16, 2016, http://docs.house.gov/meetings/AS/AS26/20160316/104553/HHRG-114-AS26-Wstate-RogersM-20160316.pdf.

6 Ashton Croft and Peter Apps, "NATO websites hit in cyber attack linked to Crimea tension," March 16, 2014, http://www.reuters.com/article/us-ukraine-nato-idUSBREA2E0T320140316.

7 Lulu Chang, "Anonymous is Behind Those Massive Cyberattacks in Turkey," *Digital Trends*, December 27, 2015, accessed April 24, 2016, http://www.digitaltrends.com/computing/anonymous-behind-turkey-cyberattakcs/.

8 Carmen-Christina Cerlig, "Cyber Defence in the EU," European Parliamentary Research Service, October 2014, at p. 3, http://www.europarl.europa.eu/EPRS/EPRS-Briefing-542143-Cyber-defence-in-the-EU-FINAL.pdf; see Kim Willsher,"French fighter plans grounded by computer virus," *Telegraph,* February 7, 2009, accessed April 24, 2016, http://www.telegraph.co.uk/news/worldnews/europe/france/4547649/French-fighter-planes-grounded-by-computer-virus.html.

year period and that such "intrusions . . . posed a threat to U.S. military operations."[9] Similarly, the targeting and exploitation of Defense Industrial Base companies' networks has resulted in the wholesale theft of US intellectual property valued at billions of dollars.[10] Further to this point, there have been similar rampant cyber theft activities in transatlantic partner nations; a study of the cost of cyber crime in the United Kingdom in 2011 put the then annual cost at 29 billion pounds, with an "estimated cost of £21bn . . . from high levels of intellectual property theft and espionage."[11]

- Similarly, critical war-supporting infrastructures are also at high risk. The Director of National Intelligence has testified, for example, that "Russia is assuming a more assertive cyber posture based on its willingness to target critical infrastructure systems"[12] Admiral Rogers has testified that "we have seen cyber actors from more than one nation exploring the networks of our nation's critical infrastructure—and can potentially return at a time of their choosing."[13] Earlier, he testified "We have also observed that energy firms and public utilities in many nations (including the United States) have had their networks compromised by state cyber actors."[14]
- Specific examples of attacks on critical infrastructures include the Iranian distributed denial of service (DDoS) attacks on the critical infrastructure services institutions of the US and other western powers.[15] Moreover, there has been a steady and dangerous "uptick" in cyber-attacks causing physical effects. The Shamoon virus attack on Saudi Aramco in 2012, which destroyed thousands of computers,[16] and last year's Black Energy virus attack on the Ukrainian power grid which shut down portions of the grid,[17] are just two examples of these trends.

From a warfighting perspective, we have also seen the integration and synchronization of cyberspace capabilities as part of an adversary's attack strategy leading up to and in conflict. This hybrid warfare approach of blending conventional, special operations and cyber operations capabilities is most evident in conflicts in Crimea, Syria, and Iraq, and foreshadows the type of warfighting challenge that NATO will face.[18] The DNI has noted the potential for expanded cyber hybrid action in the future, stating, "Russian cyber actors, who post disinformation on commercial websites, might seek to alter online media as a means to influence public discourse and create confusion."[19] More direct attacks as part of hybrid warfare are also possible as cyber warfare integration enables adversaries to strike early and steal advantage through a variety of actions. These include the use of ransomware[20] to hold NATO assets at risk, DDoS to interrupt NATO command and control (C2) and interoperability, and physical disabling of electrical power generation and communications rendering militaries ineffective and worse, threatening domestic public safety.[21]

9 Senate Armed Services Committee, "Inquiry into Cyber Intrusions Affecting U.S. Cyber Command Contractors (2014)," 2014, p. viii, http://www.armed-services.senate.gov/imo/media/doc/SASC_Cyberreport_091714.pdf

10 John McCain, "Opening statement by SASC Chairman at hearing on U.S. maritime strategy in Asia-Pacific," Senate Armed Services Committee, September 17, 2015, http://www.armed-services.senate.gov/imo/media/doc/9-17-15%20Asia-Pacific.pdf.

11 Office of Cyber Security and Information Assurance in the Cabinet Office (UK) and Detica, "The Cost of Cyber Crime," (2011), p. 2, https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/60943/the-cost-of-cyber-crime-full-report.pdf.

12 James Clapper, "Worldwide Threat Assessment of the US Intelligence Community," House Permanent Select Committee on Intelligence, February 25, 2016, https://www.dni.gov/files/documents/Newsroom/Testimonies/HPSCI_Unclassified_2016_ATA_SFR-25Feb16.pdf.

13 Admiral Michael S. Rogers, "Statement before the Subcommittee on Emerging Threats and Capabilities," House Armed Services Committee, March 16, 2016, http://docs.house.gov/meetings/AS/AS26/20160316/104553/HHRG-114-AS26-Wstate-RogersM-20160316.pdf.

14 Rogers, September 29, 2015 testimony, op. cit.

15 Thomas Fox-Brewster, "U.S. Accuses 7 Iranians of Cyberattacks On Banks and Dam," *Forbes*, March 24, 2016, accessed May 4, 2016, http://www.forbes.com/sites/thomasbrewster/2016/03/24/iran-hackers-charged-bank-ddos-attacks-banks/#7a53014f7f8d.

16 Phil Stewart "'Shamoon' virus most destructive yet for private sector, Panetta says," Reuters, October 11, 2012, accessed April 21, 2016. http://www.reuters.com/article/us-usa-cyber-pentagon-shi-moon-idUSBRE89B04Y20121012.

17 Eduard Kovacs, "Black Energy Malware used in Ukraine Power Grid Attacks," *Security Week*, January 4, 2016, accessed April 21, 2016, http://www.securityweek.com/blackenergy-group-uses-destructive-plugin-ukraine-attacks.

18 Michael Kofman "Russian Hybrid Warfare and Other Dark Arts," *War on the Rocks*, March 11, 2016, accessed April 21, 2016, http://waronthe-rocks.com/2016/03/russian-hybrid-warfare-and-other-dark-arts/.

19 James Clapper, "Worldwide Threat Assessment of the US Intelligence Community," Senate Armed Services Committee, February 9, 2016, p. 2, http://www.armed-services.senate.gov/imo/media/doc/Clapper_02-09-16.pdf.

20 Ransomware is virus software that blackmails users by encrypting their hard drives or locking them out of the computer. It then demands payment to restore it. Definition from PCMag.com.

21 Because of the frequently poor state of cyber security, many of such attacks could be successful without the need for sophisticated attack capabilities.

Current Actions

NATO currently recognizes cyber-attack as a potential Article 5 trigger,[22] and also has recognized the necessity to defend its own networks while, for the most part, leaving the defense of nations to the nations themselves. NATO has created a small Cyber Response Team to assist nations that request help. NATO's Multinational Cyber Defense Capability Program has developed work packages for the sponsoring nations of Canada, the Netherlands, and Romania that permits sharing of information within a trusted community and is working on other capabilities.[23] NATO's Cooperative Cyber Defense Center of Excellence, based in Estonia, has a "mission to enhance the capability, cooperation and information sharing among NATO, its member nations and partners in cyber defense by virtue of education, research and development, lessons learned and consultation."[24] Among other activities, it hosts valuable cyber exercises such as Locked Shield, which includes national and NATO cyber teams.[25]

Numerous analyses, as well as the incidents noted above and the continued significant number of cyber-attacks daily, demonstrate the potential for significant cyber operations used as a facilitator or attack vector leading up to and including in conflict. NATO's recognition of cyber-attacks as a potential Article 5 trigger is an affirmation of the challenge.[26] Moreover, while one of NATO's strengths is the interoperability of the different national forces, without a cyber framework or operational partnerships cyber vulnerability at the national level could mean that neither the NATO command authorities nor other nations could safely interoperate with a vulnerable entity, for example, having its communications compromised.

> Without a cyber framework or operational partnerships cyber vulnerability at the national level could mean that neither the NATO command authorities nor other nations could safely interoperate with . . . vulnerable [national forces]. . .

The United States is recognized as having high-end cyber capabilities, and has undertaken numerous steps including the establishment of Cyber Command.[27] Cyber Command's forces not only include active duty, but National Reserve and Guard Forces.[28] Forces are being aligned to support protection of DoD networks; providing options to warfighting commanders for better meeting warfighting and deterrence objectives; and protection of national critical infrastructure from attacks of significant consequence. Cyber Command intends to stand-up over 130 teams with up to 6,200 professionals to support these functions.[29]

US National Guard Cyber Forces directly support states, but are standing up to support Cyber Command's cyber protection team mission.[30] These cyber Guard units

22 NATO, "Wales Summit Declaration," September 5, 2014, para. 72, http://www.nato.int/cps/ic/natohq/official_texts_112964.htm. Importantly, at the 2014 Wales Summit, NATO members agreed that there is no distinction (in terms of a NATO decision to respond) between a physical and cyber-attack.

23 NATO, Cybersecurity: Home page, http://www.natolibguides.info/cybersecurity; Multinational Cyber Defense Capability Development, https://mncd2.ncia.nato.int/Pages/default.aspx.

24 See, NATO Cooperative Cyber Defense Centre of Excellence, https://ccdcoe.org/.

25 NATO Cooperative Cyber Defense Centre of Excellence, "Locked Shields 2015," April 20, 2015, https://ccdcoe.org/locked-shields-2015.html. The 2016 Locked Shield exercise is described as "World's largest international cyber-defence exercise underway in Tallinn," SC Magazine, April 20, 2016, http://www.scmagazine.com/worlds-largest-international-cyber-defence-exercise-underway-in-tallinn/article/490938/?utm_campaign=ThreatScape+Media+Highlights&utm_source=hs_email&utm_medium=email&utm_content=28725283&_hsenc=p2ANqtz-96YQ52qgo6y4bYoUisCZW-shGt1M1DjI0hEW804dfp4J425hvo0dxF6NF3xPydwNWG5lLL-KU1T3rIZ4R2CXgFnSoP4_SdKsw9X45w1repbDFu4qUOU&_hsmi=28725283.

26 Wales Summit Declaration, September 5, 2014, op. cit., para. 72.

27 Deputy Secretary of Defense Robert O. Work, "Opening Statement Before the Senate Armed Services Committee," Senate Committee On Armed Services, September 29, 2015, http://www.armed-services.senate.gov/imo/media/doc/Work_09-29-15.pdf.

28 Christopher R. Quick, "Creating a Total Army Cyber Force: How to Integrate the Reserve Component into the Cyber Fight," *Land Warfare Papers*, The Institute of Land Warfare, Association of the United States Army, September 2014, accessed April 24, 2016, (7), http://www.ausa.org/publications/ilw/DigitalPublications/Documents/lwp103w/offline/download.pdf.

29 Admiral Michael S. Rogers, Commander, United States Cyber Command, "Statement Before The Senate Committee On Armed Services, Senate Committee On Armed Services, March 19, 2015, p. 7, https://fas.org/irp/congress/2015_hr/031915rogers.pdf

30 "Guard Names Sites of Cyber Units," *NGAUS*, December 15, 2015, accessed April 21, 2016, http://www.ngaus.org/newsroom/news/

pool talent from some of the best industry critical infrastructure providers in the nation. As the Secretary of Defense recently stated, "It brings in the high-tech sector in a very direct way to the mission of protecting the country . . . And we're absolutely going to do more of it."[31]

Some other countries, such as the United Kingdom, have also taken substantial steps in the cyber arena.[32] In 2014, the UK inaugurated the new Computer Emergency Response Team (CERT-UK) to coordinate their national response to significant cyber incidents. According to the Rt Hon Francis Maude, "CERT-UK has played a significant role [already] in protecting the Commonwealth Games and the NATO Summit in Wales from cyber threats."[33] In a similar fashion to the US approach, the UK is also developing a joint cyber reserve, which leverages the country's industry expertise and talent for national security. The UK Ministry of Defense stated that the "creation of the Joint Cyber Reserve will represent a significant increase in the number of reservists employed in cyber and information assurance."[34]

However, cyber capabilities are not uniformly available to all NATO nations. In March 2010, "NATO and the European Union warned that the number of successful cyber-attacks against their networks" had increased significantly over the past year.[35] More recently, in light of the attack on the Ukraine power grid, "researchers studying the attacks say the malware believed responsible – a new version of the so-called BlackEnergy bug – has likely spread to numerous European power grids and is poised to infect many more."[36] In short, as the discussion of the multiplicity of cyber-attacks demonstrates, the degree of protection to the telecommunications infrastructure and to the electrical grid, as two of the key critical infrastructures and particularly relevant to military operations, is, at best, quite uncertain. Such vulnerabilities undercut NATO's deterrent and defense capabilities and even invite preemptive attack. As Admiral Rogers has testified,

> if we cannot defend the infrastructure that undergirds our DoD bases and forces from foreign-based cyber threats, then our nation's military capabilities are weakened and all our instruments of national power diminished. That leaves our leaders with a need for additional options to pursue short of open hostilities, and with fewer capabilities in an actual clash of arms. This raises risk for all by inviting instability and miscalculation.[37]

Extended Deterrence and Cyber

In addition to the steps NATO is currently taking or proposing, the extended deterrence doctrine, if applied to cyberspace, could significantly ameliorate NATO's cyber vulnerabilities and deficiencies at the national level. While generally considered as a nuclear defense concept, "extended deterrence . . . serves to reassure our . . . allies of their security against regional aggression."[38] In applying that doctrine to cyber defense, nations with greater capabilities would help provide less capable nations with the establishment, transfer, training, and support of key cyber capabilities. These capabilities would be particularly focused on the protection of military networks, telecommunications infrastructure, and the electrical grid, and to provide an offensive capability to be utilized as authorized including as part of an integrated defense in a conflict.

To do this effectively, NATO should take the following actions.

guarded-names-sites-cyber-units.

31 Andrea Shalal, "U.S. National Guard may join cyber offense against Islamic State: Carter," Reuters, March 6, 2016, http://www.reuters.com/article/us-usa-military-cyber-idUSKCN0W70UQ.

32 James Blitz, "UK becomes first state to admit to offensive cyber attack capability," *Financial Times*, September 29, 2013), http://www.ft.com/intl/cms/s/0/9ac6ede6-28fd-11e3-ab62-00144feab-7de.html#axzz42b6lZylF.

33 Cabinet Office, National Security and Intelligence and The Rt Hon Lord Maude of Horsham "UK Cyber Security Strategy: Statement on Progress 3 Years On," December 11, 2014, accessed April 24, 2016. https://www.gov.uk/government/speeches/uk-cyber-security-strategy-statement-on-progress-3-years-on.

34 "New Cyber Reserve Unit Created," Ministry of Defence, Joint Forces Command, September 29, 2013, accessed April 21, 2016, https://www.gov.uk/government/news/reserves-head-up-new-cyber-unit.

35 "Examining the Cyber Threat to Critical Infrastructure and the American Economy," Hearing before the Subcommittee on Cybersecurity, Infrastructure Protection, and Security Technologies of the Committee on Homeland Security, House of Representatives, March 16, 2011, p. 40, accessed April 24, 2016, https://www.gpo.gov/fdsys/pkg/CHRG-112hhrg72221/pdf/CHRG-112hhrg72221.pdf.

36 Doug Bernard, "National Power Grids Increasingly Targeted in Cyber Attacks," February 1, 2016, http://www.voanews.com/content/national-power-grids-increasingly-targeted-in-cyber-attacks/3171551.html.

37 Statement of Admiral Michael S. Rogers, Before the Senate Committee On Armed Services, September 29, 2015, op. cit., p. 8.

38 Department of Defense, "Quadrennial Defense Review 2014," p. v, http://archive.defense.gov/pubs/2014_Quadrennial_Defense_Review.pdf.

- Create "cyber framework nations," each of which could help support national capabilities including the establishment, transfer, training, and support of necessary cyber capabilities in line with the framework nation concept approved by NATO at the 2014 Wales summit. For example, a cyber framework nation could help a less cyber-capable ally establish an effective intrusion protection system, provide forensic support, and develop resilience capabilities to be utilized in the event of attack by an adversary. The United States would be the first cyber framework nation;
- Establish operational partnerships with key private entities, including ISPs and power grid operators. For example, military, telecommunications, and electrical grid operators could create, in advance, capabilities that would mitigate a Tier V or VI attack. As discussed below, this should be done first at the national level; the US, as a cyber framework nation, could help others organize for this effort; and
- Develop doctrine and capabilities to provide for the effective use of cyberspace in a conflict as part of NATO's warfighting capabilities. For example, cyber tools potentially could disrupt an adversary's communications, logistics, and sensors or be utilized as part of a defense of critical infrastructures.

An Approach for Building New NATO Cyber Capability–the Cyber Framework Nation

Upgrades to the national military, telecommunication, and power grid infrastructure networks of the NATO Allies should provide for both organic defense and resilience capabilities. The US National Institute of Standards and Technology recently developed a national cybersecurity framework (CSF), which leverages best practices and international standards.[39] There are five different functions of the CSF: identify, protect, detect, respond, and recover. A cyber framework country can help provide highly scalable capabilities in each of these functions. These include:

- First, identifying highest priority national military cyber assets and supporting telecom and power grid networks that would need to be protected or employed in an Article 5 response to a cyber-attack by an adversary.
- Second, extending/enhancing automated intrusion protection and developing resilience efforts, starting with data classification and segmentation, to participating NATO member nations' militaries, telecommunication companies, and electrical grids. Utilize high-end protection capabilities, such as multi-factor authentication, end-to-end data encryption and diverse, redundant networks, to ensure best information assurance practices in data confidentiality, integrity, and availability.
- Third, increasing detection capabilities by provisioning shared cyber threat intelligence capabilities. A NATO cyber threat intelligence capability would develop and share cyber indications and warnings regarding the movement of high-end state cyber-threat activity towards NATO networks and information assets.[40]
- Fourth, development of NATO cyber defense "playbooks" and training exercises for cyber-attack response, with techniques, tactics, and procedures (TTPs) developed to maximize the value of the defense and resilience capabilities noted above. Include national grid and telecommunications partners in the private sector as part of the playbook TTPs and training exercises.
- Fifth, providing "fly away" cyber-warfare teams to provide NATO member states' "blue team" assistance to "operate in degraded environments," recover, and support malware forensics. These would be complementary to NATO Cyber Response Teams.

Nations should create a "cyber conflict coordination board" that would coordinate with NATO and the EU to provide the necessary guidance and operational activities for national military, telecommunication, and electrical grid infrastructures. The focus would be on requirements for a conflict, both conventional and hybrid. Membership would consist of, minimally, the national ministry of defense, the key telecommunication companies, and the key electrical grid providers; the nation would decide on any other governmental and/or private sector entities. However, as the board is

39 NIST Cybersecurity Framework, "FAQs," http://www.nist.gov/cyberframework/cybersecurity-framework-faqs-framework-basics.cfm (includes Framework and Frequently Asked Questions).

40 NATO could develop a new arrangement or potentially utilize existing assets such as the NATO Intelligence Fusion Center. The key would be very prompt action to share information.

intended to be able to be an operational entity to provide guidance in a conflict (as well as before), membership should be established on a functional basis and limited to those absolutely necessary to the task.

Initially, the cyber framework nation can help to establish or enhance an existing national framework. Over time, simulations, exercises, and information sharing will help direct and prioritize other efforts by exposing gaps and opportunities. Joint exercises, when effective, usually result in some degree of information sharing. Explicit and incidental information sharing, especially between private and public sector partners, will be a critical requirement if operational protection and/or resilience is to be achieved. Each country should pick a model it finds compatible, but the keys are a combination of speed and full interchange. In the US, one of the most effective models is the "Information Sharing and Analysis Center (ISAC) a nonprofit organization that provides a central resource for gathering information on cyber threats to critical infrastructure and providing two-way sharing of information between the private and public sector."[41] ISACs are typically developed around a critical infrastructure sector, such as the electrical grid or telecommunications sectors. The Financial Services ISAC is often considered the greater among equals, as it has a highly automated system for rapid cyber threat information exchange.

The cyber framework nation model can be particularly valuable in the context of hybrid warfare. Hybrid warfare certainly may involve cyber-attacks, but it also can include various types of issues involving law enforcement and related activities such as border control. A cyber framework can be utilized to promote military and Law Enforcement Agency (LEA) cyber coordination within a nation and across borders. Militaries and LEAs have often worked very closely in post-conflict crises or natural disaster situations. Under the cyber framework nation lead, NATO nations could leverage related cybersecurity military-LEA efforts across borders; contribute customs, law enforcement, military, and other security experts and assets to cyber framework nation-led cyber exercises; and working with member states, improve their response and recovery capacity to and from cyber-attacks.

As noted above, to accomplish effective cyber defense and resilience will require working with key private entities within a nation, including, as suggested above, with relevant ISPs and electrical grid operators. NATO can enhance these national efforts by expanding its activities with the private sector to promote greater resiliency in the power grid and telecommunication sectors. For the power grid, transatlantic service territory companies like National Grid could be a strong coordinator and collaborator in this space. In the telecommunications world, a partnership with North American Network Operators Group (NANOG)—a transatlantic organization that was deeply involved in countering Russian cyber aggression against Estonia, or a company with a comprehensive security interest in the European telecommunications infrastructure and nationally aligned in support of NATO, could provide similar collaboration and coordination in strengthening European ISP resilience. Taking steps in advance and exercising to develop coordinated capabilities in the event of an attack will enhance resiliency. Broad, geopolitical resiliency requires coordination, not just within nations but also with multi-national service providers.[42]

At the supranational level, NATO and the EU could extend their current coordination to provide collaborative guidance and operational efforts. Many of the technical aspects of ensuring that twenty-eight nations maintain integrated approaches have been resolved in various NATO efforts such as Battlefield Information Collection & Exploitation Systems (BICES), which have been utilized in multiple circumstances, and the BICES approach could provide a channel to ensure that the different framework nations provide interoperable solutions.[43]

Resources and Costs for a Cyber Framework Approach

Most of the activity described above, including the development of cyber frameworks, requires only modest investment and can be scaled at a relatively low cost. For example, military system and network configuration guidance, once developed, need not be significantly redesigned to apply elsewhere. Similarly, development of realistic exercise scenarios

41 Wikipedia, "Information Sharing and Analysis Center," https://en.wikipedia.org/wiki/Information_Sharing_and_Analysis_Center.

42 Exercises should include circumstances where allied access to networks is degraded, and as the text suggests, resilience for civilian capabilities will be critical.

43 Glynne Hines, BICES Group Executive Director, "Building Capabilities for Multinational Interoperability in an Era of Austerity" http://www.afei.org/PE/4A05/Documents/Glynne%20Hines_final%20presentation(approved).pdf.

or playbooks requires little redesign to be useful to another nation. Countries adopting the baseline configuration guidance discussed above could also benefit by customized vulnerability and compliance scanning tools that are available.

From a US perspective, the National Guard has long undertaken partnership programs as part of the Department of Defense's international security functions. While only one National Guard unit is currently supporting other nations in cyber (175th ANG unit—Baltimore, MD),[44] an expanded use of the US Guard (or UK Joint Cyber Reserve) could provide a backbone element for a US- (or UK-) led framework nation approach at a reasonable cost. In fact, the US National Guard is training cyber teams in the protection of industrial control systems, one such team being Washington state's 262nd Network Warfare Squadron.[45] These small, but capable cyber protection teams could be used not only for defense of US critical infrastructure, but in support of cyber protection to NATO military and critical infrastructure networks. Further, he use of private contractor support, as is currently being undertaken for implementation and operations services of the NATO Communications and Information Agency in support of its training and analysis programs,[46] or for the actual defense of NATO networks, could enhance such an approach.

These small, but capable cyber protection teams could be used not only for defense of US critical infrastructure, but in support of cyber protection to NATO military and critical infrastructure networks.

Most importantly, the costs associated with a cyber framework approach should not be overly substantial especially compared to other defense projects and considering the potential impact of the high degree of vulnerability that NATO nations face. By way of comparison, NATO has entered into two contracts for the defense of NATO networks: according to public reports, the first, in 2012, was for 50 million euros,[47] and the second was in 2015 for 19 million euros.[48] While such contracts undoubtedly do not cover all costs associated with the defense of networks, nonetheless funding for national cyber resilience utilizing a framework nation approach, as suggested above, should be on a comparable order of magnitude, which would be well within the financial capabilities of NATO and the framework and receiving nations. While there would be multiple ways in which to work out funding requirements, a potentially useful approach would be for NATO and the European Union to collaborate in this arena. Most specifically, extending the recent NATO-EU cyber collaboration, the European Union could create a "cyber reliability support initiative" that would help fund upgrades to national military, telecommunications, and electrical grid infrastructures to enhance cyber resilience.

Cyber Offensive Doctrine and Capabilities

NATO needs to develop doctrine and capabilities to provide for the effective use of cyberspace in a conflict as part of NATO's warfighting capabilities. Cyber capabilities have the prospect of being an asymmetric capacity and force multiplier that could be of important consequence to the defense of NATO nations.

In the event of a substantial conventional attack against the Baltic nations, for example, local force ratios could favor the attacker. Cyber and other capabilities, such as electronic warfare and special operations forces, could be important to enhance NATO's initial defenses and to

44 Wikipedia, "Maryland-Estonia National Guard Partnership," https://en.wikipedia.org/wiki/Maryland%E2%80%93Estonia_National_Guard_Partnership.

45 24th Air Force Public Affairs, "24th Air Force Commander visits Washington ANG units," May 22, 2014, http://www.24af.af.mil/News/Article-Display/Article/731780/24th-air-force-co.

46 "Booz Allen Selected by the NATO Communications and Information Agency to Provide Analysis, Training and Program Support for up to Three Years," *New York Times*, March 1, 2016, http://markets.on.nytimes.com/research/stocks/news/press_release.asp?docTag=201603010945BIZWIRE_USPRX____BW6292&feedID=600&press_symbol=27445532.

47 Andrea Rothman, Finmeccanica Says NATO Contract Is Gateway for More Cyber Work, March 1, 2012, http://www.bloomberg.com/news/articles/2012-03-01/finmeccanica-says-nato-contract-is-gateway-for-more-cyber-work.

48 Leonardo/Finmeccanica, "Finmeccanica Awarded €19M to Extend Successful NATO Cyber Security Capability, Press Release, September 9, 2015, http://www.finmeccanica.com/en/-/nato-cyber-security-sicurezza.

deal with the prospect of an attempt by an adversary at precluding reinforcement through anti-access/area denial efforts. Cyber, for example, could have impact on an adversary's communications, logistics and sensors.[49] Moreover, cyber-attack capabilities potentially can have a role in providing defense of national networks.

NATO already has such doctrine relating to electronic warfare, and cyber warfare has many similarities.[50] In a similar fashion to air campaign planning, prior analysis of targets, including the probability of collateral consequences could be undertaken, enabling the development of cyber-attack "campaign packages" for commanders. Providing such capabilities to a defending force would have significant military value. Moreover, as CSIS' James Lewis has stated,

> Adding offensive cyber capabilities to NATO's force structure and response doctrine will increase its deterrent capabilities . . . [A] clear enunciation of how NATO would use offensive cyber capabilities as part of any defensive operation would also change opponents' risk calculations in ways that would force them to consider how offensive actions, even if intended to be covert, are not free of risk or cost.[51]

Cyber capabilities have the prospect of being an asymmetric capacity and force multiplier that could be of important consequence to the defense of NATO nations.

On the other hand, a failure of an opponent to understand that cyberspace is a factor for NATO could lead to "miscalculating as they consider the risks of using force or coercion against NATO members or interests."[52] Deterrence depends heavily on perceptions of capabilities, and NATO should not fail to show that it will use cyber offensive capabilities as appropriate in order to enhance deterrence. To do otherwise is an open invitation to an aggressor that would just confirm any conclusions drawn that active coercion against neighbors to achieve strategic gains will entail little long-term cost. Any countermeasures, cyber or conventional, that NATO and/or individual nations take in response to the threat will directly impact the risk calculus of any adversary.

The United States, which has the leading military capability in NATO, has a declared cyber offensive doctrine. As stated in the DoD Cyber Strategy,

> "[I]f directed by the President or the Secretary of Defense, DoD must be able to provide integrated cyber capabilities to support military operations and contingency plans. There may be times when the President or the Secretary of Defense may determine that it would be appropriate for the U.S. military to conduct cyber operations to disrupt an adversary's military related networks or infrastructure so that the U.S. military can protect U.S. interests in an area of operations. For example, the United States military might use cyber operations to terminate an ongoing conflict on U.S. terms, or to disrupt an adversary's military systems to prevent the use of force against U.S. interests."[53]

In fact, the Secretary of Defense has publicly stated that the US is using that capability in the context of the coalition conflict against the Islamic State of Iraq and al-Sham (ISIS or ISIL), saying "We're also using cyber tools to disrupt ISIL's ability to operate and communicate over the virtual battlefield."[54] Of course,

49 See James A. Lewis, "The Role of Offensive Cyber Operations in NATO's Collective Defense," Tallinn Paper No 8, 2015, p. 4, at https://ccdcoe.org/sites/default/files/multimedia/pdf/TP_08_2015_0.pdf: ("the most likely form of attack will be against command and control systems (including sensors and computer networks) and against the software that runs advanced weapons such as surface-to-air missiles or fighter aircraft").

50 The US Army has combined its cyber and electronic warfare doctrine in "FM 3-38, Cyber Electromagnetic Activities," Department of the Army, February 2014, http://armypubs.army.mil/doctrine/DR_pubs/dr_a/pdf/fm3_38.pdf.

51 James A. Lewis, "The Role of Offensive Cyber Operations in NATO's Collective Defense," op. cit., pp. 2, 7.

52 Ibid.

53 The DOD Cyber Strategy, p. 5 (2015), op. cit.; The Air Force recently issued a cyber policy including the role of cyber offense. Air Force Policy Directive 17-2, Cyberspace Operations, April 11, 2016.

54 Secretary Carter and Gen. Dunford "Department of Defense Press Briefing by Secretary Carter and Gen. Dunford in the Pentagon Briefing Room," February 29, 2016, http://www.defense.gov/News/News-Transcripts/Transcript-View/Article/682341/department-of-defense-press-briefing-by-secretary-carter-and-gen-dunford-in-the.

many members of the coalition are NATO allies. Going forward, NATO nations should use the current counter-ISIS approach for integrated cyber capacity as part of NATO collective defense planning for future NATO campaigns.

Cyber defense and resilience likely would also play an important role in the event of any hybrid conflict. A hybrid attack could involve targeting critical infrastructure, both for immediate effect or as preparation for a follow-on conventional effort. As noted above, however, developing resilience, including through the use of cyber framework nations, would be an important factor both to deterring and to responding to such cyber hybrid attacks. Moreover, during heightened tensions and prior to conflict, NATO's cyber capabilities could be integrated as flexible deterrent options (FDO) packages. Nations under propaganda onslaught that affects their security have the legal authority to block such actions. Malware inserted into networks can be removed, and command and control disabled, just as mines in territorial waters can be eliminated. An adversary who utilizes short-term cyber actions such as disabling a power grid for several hours or undertaking a blocking DDoS attack can properly face appropriate cyber responses. For example, attributed (i.e., traceable) web crawling and/or attributed denial-of-service actions against an adversary's force generation capabilities could be integrated as FDOs to help dissuade adversaries to take further escalatory action.

To be sure, there are certainly issues regarding the use of cyber offensive capabilities in a conflict or prior to conflict in a hybrid circumstance that need to be carefully considered, such as release authority and, as noted above, considerations of potential collateral damage. However, NATO has developed sensitive doctrine and capabilities in other arenas such as nuclear. It might follow that approach by utilizing, and if necessary expanding, the mandate of the Cyber Defence Committee, which reports to the North Atlantic Council (akin to what is done for the Nuclear Planning Group), and also authorizing, under appropriate mandate, for the Supreme Allied Commander Europe and Supreme Allied Commander Transformation to develop cyber doctrine and planning.

* * *

A final point: cyber extended deterrence is not a gift from the United States or other cyber-capable countries to less capable recipients. If the US were to fight forward and with allies, as all US military doctrine and plans expect, then it would be extraordinarily hard to do so in an era of networked warfare without the military, telecommunications, and power grids of host nations being available for US and allied activities.

Cyber vulnerabilities are one of NATO's and its member-states' most significant challenges, but an extended deterrence approach as recommended could significantly and promptly reduce such vulnerabilities.

Franklin D. Kramer is a distinguished fellow and on the board at the Atlantic Council and a former assistant secretary of defense.

Robert J. Butler is an adjunct fellow at the Center for a New American Security and served as the first US Deputy Assistant Secretary of Defense for Cyber Policy.

Catherine Lotrionte is the Director of the CyberProject in the School of Foreign Service at Georgetown University and former Counsel to the President's Foreign Intelligence Advisory Board and former Assistant General Counsel at the Central Intelligence Agency.

Atlantic Council Board of Directors

Atlantic Council

The Atlantic Council is a nonpartisan organization that promotes constructive US leadership and engagement in international affairs based on the central role of the Atlantic community in meeting today's global challenges.

Atlantic Council

1030 15th Street, NW, 12th Floor,
Washington, DC 20005

(202) 463-7226, www.AtlanticCouncil.org