June 2019

Perspective
EXPERT INSIGHTS ON A TIMELY POLICY ISSUE

LILLIAN ABLON, ANIKA BINNENDIJK, QUENTIN E. HODGSON, BILYANA LILLY, SASHA ROMANOSKY, DAVID SENTY, JULIA A. THOMPSON

Operationalizing Cyberspace as a Military Domain

Lessons for NATO

Defense of the North Atlantic Treaty Organization (NATO) in cyberspace requires an understanding of the threats the alliance must face, knowing where it must act, and ensuring that the alliance has the capabilities and capacity available to successfully defend itself. Since the end of the Cold War, NATO has expanded its reach not only in terms of membership and partners, but also in terms of its operations. As a globally engaged organization, NATO must be prepared to address cyber threats that emanate from anywhere in the world. Truly integrating cyber operations into the alliance requires broadly educating the members of the alliance on operations in cyberspace; cyber operational planning, training, and exercises to create the "muscle memory" necessary; and rigorously assessing lessons learned as they emerge.

At the June 2016 Defense Ministerial Meeting, the NATO Defense Ministers agreed to recognize cyberspace as an operational domain, and that decision was endorsed and reaffirmed at the NATO Summit in Warsaw in July 2016. As part of this effort, NATO directed the development of an implementation roadmap for

RAND
CORPORATION

review in the February 2017 Defense Ministerial Meeting, and it was subsequently approved.

NATO's Allied Command Transformation (ACT) requested the RAND Corporation's assistance to provide analysis that would inform domain implementation through the execution of the roadmap tasks, focusing on identifying lessons learned from national practice; to conduct analysis and engagement to develop, refine, and improve material to inform NATO decisionmaking; and to provide an independent, objective view on approaches to implement the roadmap.

This Perspective leverages insights from that focused analytic effort; additional research in such open-source literature as official government documents; and interviews with current and former officials and cybersecurity practitioners to provide additional commentary, which we hope is suitable for a wider audience. In particular, we discuss three viewpoints relevant to this endeavor upon which NATO is embarking by focusing on NATO's *past*, *present,* and its *emerging* position in cyberspace.

First, we examine a period in NATO's history when it had similarly faced new challenges and when the alliance was forced to adapt to new missions. Specifically, we focus on the aftermath of the September 11, 2001, attacks on the United States, when NATO sought to enhance its ability to address potential attacks with chemical, biological, radiological, and nuclear (CBRN) weapons. Despite national-level political differences, Supreme Headquarters Allied Powers Europe (SHAPE) was able to translate concepts into capability, including through the use of exercises to validate and fine-tune them by leveraging the niche skills and expertise of key member states—particularly the Czech military. We also briefly identify the development of the International Security Assistance Force's (ISAF's) Afghan Partner Network as a separate case of NATO adaptation that highlights the ability of NATO military leaders to drive innovative improvements to information-sharing during coalition operations.

Second, we discuss current efforts by NATO to consider and adapt its structure, forces, systems, and processes to prepare itself for integrating cyberspace as an operational domain. The disparity in cyber capabilities across the alliance, as well as the highly classified nature of some of the members' capabilities, makes this more difficult, but not impossible, to achieve. While cyber presents technical problems, we believe that integrating cyberspace into the alliance should start with addressing foundational planning along at least three key areas: defining cyberspace functions to operationalize the domain, building exercises and training programs (including developing and maintaining the supporting infrastructure), and developing a cyber workforce. Further, for cyberspace to truly be an enduring mission, NATO must ensure that not only are the technical capabilities (e.g., NATO Computer Incident Response Capability [NCIRC]) on continual alert, but also that the military assets are constantly exercising the functions described previously.

Finally, while there are many challenges to successfully operating in cyberspace, we examine one particular capability, indications and warning (I&W), that all nations should develop to maintain and ensure an effective military presence within cyberspace. Cyber I&W is the practice of collecting actionable information about threats to cyberspace that may provide early detection and warning of impending malicious cyberactivity. It includes prioritizing essential assets, recognizing emerging threats, and enumerating technical and behavioral indications of imminent hostile activity. It is also a relatively new capability for all modern nations and military alliances, and, in the following discussion, we examine some of the existing scholarship and adapt a leading framework for the NATO context.

Learning from NATO's Past: An Adaptable Alliance

In identifying cyberspace as a new operational domain, NATO has taken a major step in adapting in response to emerging threats. Such change is not without challenges, but neither is it without precedent. In 2002, NATO began institutionalizing new capabilities and expertise so that it could rapidly address CBRN threats. As observers reported at the time, such "agile and specialized forces previously were alien to NATO operations."[1] Some of the lessons learned from NATO's successful development of these new capabilities are relevant as the alliance seeks to realize the goals in its new cyber strategy through new expertise, capabilities, doctrine, and structures. Specifically, NATO took proactive steps during the development of its CBRN capabilities to hone and reinforce concepts through exercises and training, to incorporate diverse levels of capability within the alliance, and to integrate CBRN into military doctrine and planning. NATO's development of CBRN capabilities provides useful insights for future alliance work in the cyber domain.

Abbreviations

ACT	Allied Command Transformation
CBRN	chemical, biological, radiological, and nuclear
CERT	Computer Emergency Response Team
CHODS	Chiefs of Defense Staff
COE	Center of Excellence
COPD	*Comprehensive Operational Planning Directive*
CyOC	Cyber Operations Center
DGP	Defense Group on Proliferation
EU	European Union
IOC	initial operating capability
ISAF	International Security Assistance Force
I&W	indications and warning
JAT	Joint Assessment Team
NATO	North Atlantic Treaty Organization
NBC	nuclear, biological, chemical
NDPP	NATO Defense Planning Process
NCIRC	NATO Computer Incident Response Capability
SHAPE	Supreme Headquarters Allied Powers Europe
SPS	Science for Peace and Security
TTPs	tactics, techniques, and procedures
WMD	weapon(s) of mass destruction

Gradual Concept Development, Rapid Implementation

As has more recently been the case for cyberspace, NATO initially took time to develop consensus over a conceptual framework for allied defense against CBRN threats. Over a decade elapsed between the alliance's initial broad recognition of CBRN threats in its 1991 Strategic Concept and the 2003 establishment of a dedicated CBRN battalion.[2] Part of the initial challenge lay in developing a common assessment of the threat and capability gap. A two-year effort by NATO's Senior Defense Group on Proliferation (DGP) in the mid-1990s made a significant contribution by assessing the risks of weapon(s) of mass destruction (WMD) proliferation and considered the necessary capabilities and shortcomings.[3] At the 1999 Washington Summit, allies agreed to a "WMD Initiative" that, while not requiring dramatic investment of alliance resources, represented a signal of NATO intent.[4]

The September 11, 2001 attacks against the United States provided impetus for more rapid and ambitious progress on alliance capability and expertise to address CBRN challenges.[5] Labeled a transformation summit, the 2002 Prague Summit established, in the words of then–NATO Secretary General Lord Robertson, a "blueprint to improve NATO's ability to assist national authorities in protecting both civilian populations and critical infrastructure against the consequences of terrorist attacks, and particularly attacks involving chemical, biological, radiological or nuclear weapons."[6]

Implementation moved more rapidly after the Prague Summit.[7] Despite the persistence of highly politicized differences across the alliance about WMD threats, NATO as an institution was able to maintain momentum on CBRN initiatives. Over the course of the year following the Prague Summit, NATO's SHAPE had spearheaded the process of establishing a dedicated high-readiness, multinational force that could provide NATO with credible nuclear biological chemical (NBC) capability and would help to "ensure the Alliance's freedom of action in an NBC environment."[8] SHAPE identified the need to integrate NBC teams directly into NATO's military structure, proposed a NATO Multinational CBRN Defense Battalion, and initiated an efficient process lauded for its creativity and flexibility.[9] By October 2003, SHAPE had held a Force Generation conference to generate units for the battalion, and by December 2003, Secretary General Robertson had declared Initial Operating Capability (IOC) for the battalion.[10] By 2005, analysts highlighted NATO's development of an operational chemical/biological/radiological defense battalion as one of the Prague Summit's major successes.[11] Today, the multinational Combined Joint CBRN Defense Task Force, which includes a CBRN Joint Assessment Team (JAT) and the CBRN battalion, includes 21 NATO countries and is ready to rapidly deploy in armed conflict or crisis scenarios.[12] However, because NATO bureaucratic processes require that all 29 member states agree on a CBRN mission before NATO assets can be employed in the absence of an existing NATO operation, time sensitivities associated with a CBRN crisis could ultimately require that the alliance play more of a coordinating role in a coalition response involving multiple NATO members.[13]

Robust Exercise Program

NATO military authorities pursued a robust training and exercise program to hone the initial response concept (training and exercises for cyberspace are discussed more in the next section). NATO held its first CBRN training exercise soon after the Prague Summit—in November 2002—with 115 NATO troops from 19 countries divided into prototype teams to respond to NBC attacks and to operate CBRN sampling and detection laboratories.[14] Over the course of the following year, allies validated the concepts for the CBRN Event Response Team and Deployable CBRN Analytical Laboratory through a rigorous program of seven exercises for prototype teams across the Czech Republic, Spain, Canada, Italy, the United States, and the United Kingdom.[15] NATO allies continue to fine-tune CBRN capabilities through multinational exercises: In 2017, the U.S. Army's Joint Multinational Readiness Center expanded its rotational training for NATO allies and partners to include replicated mock CBRN sites at the Hohenfels training area in Germany.[16] To fully address both the civilian and military dimensions of CBRN cooperation, NATO could consider finding additional opportunities to incorporate civilian organizations into future operational exercises.[17]

At the political level, NATO has used crisis management study seminars to identify use cases for the CBRN battalion within the NATO Response Force. One such seminar, Dynamic Response '07, presented defense ministers, Chiefs of Defense Staff (CHODS), and ambassadors with scenarios—including those involving WMD use—to demonstrate the ability of the NATO Response Force to operate within a future threat environment that included CBRN threats.[18]

Expanding Skills, Knowledge and Capabilities Across a Diverse Alliance

As the alliance adapts in response to emerging security challenges, individual member states inevitably offer varying levels of relevant skills, expertise, and capabilities. As with cyber responses, effective responses to CBRN incidents require technical expertise that can diverge widely across allies and partners.[19] Many NATO member states have insufficiently invested in the niche capabilities required for CBRN response and management. Those capabilities that exist may be under civilian or military control depending on the country, necessitating robust civil-military cooperation. National gaps in technical expertise and capabilities may have concrete operational implications during a conflict.

To address the challenges associated with gaps in CBRN expertise across the alliance, NATO was able to leverage existing expertise and capabilities of key allies, including the Czech military, which had outperformed U.S. forces in the 1991 Persian Gulf war in detecting low levels of lethal nerve agents.[20] In 2003, with the Czech CBRN defense unit serving as a training and exercise host and providing core capabilities, NATO included 12 other NATO members and two partner nations in the CBRN unit to introduce and reinforce CBRN-related skills and knowledge. As one report observed, "rather than have the Czechs simply train their own battalion for rapid deployment with the NATO Response Force, NATO's new approach is to increasingly integrate one country's expertise across the borders of the alliance members."[21] Over the intervening years, the rotational nature of the Combined Joint CBRN Defense Task Force, composed of personnel from NATO countries on yearlong standby and spearheaded by rotating voluntary lead nations, has also helped to further develop expertise across the 21 NATO countries participating in the initiative.[22] The Czech-hosted CBRN training center continues to contribute to national-level training—for example, helping to train members of the Greek military in preparation for the 2004 Summer Olympics in Athens.[23]

In addition to developing alliance-specific capabilities, NATO has sought to improve national-level CBRN expertise capabilities among NATO members and partner countries. Like cybersecurity, CBRN responses fall under the jurisdiction of civilian entities in many countries, augmented by national militaries when needed, creating potential for further complications in the dissemination of skills and knowledge and coordination of alliance response.[24] One step NATO has taken to engage civilian CBRN communities is through NATO's Science for Peace and Security (SPS) Programme, which facilitates research collaboration on CRBN, including training activities and workshops.[25] Additionally, NATO's school at Oberammergau offers a range of CBRN courses for NATO member-state military and civilian personnel to support CBRN defense and exercise planning, including coursework for analysts on CBRN intelligence I&W.[26] Broad dissemination of skills and capabilities among both civilian and military entities in NATO member and partner states could help to improve national or coalition responses to a CBRN event, even if NATO as an alliance does not take on a formal leading role.[27]

Embedding New Initiatives into Doctrine, Planning, and Prediction

NATO has worked since 2002 to integrate CBRN defense into its doctrine and military planning. NATO's military strategy for terrorism, approved in 2002 at the Prague Summit, provided an initial framework for implementation of each of the summit's proposed CBRN initiatives.[28] A strategic policy for CBRN threats, published in 2009, identified "strategic enablers" for addressing proliferation challenges and mitigation, including enablers such as intelligence and information sharing, international outreach, and strategic communication.[29] NATO's Committee on Proliferation has since deemed the 2009 policy relevant to current threats and is working to implement it. This policy also serves as the basis for some allies' national strategies for CBRN defense. Member states have agreed to prioritize CBRN defense in the NATO Defense Planning Process (NDPP), allowing planners to translate gaps into concrete capability requirements.[30]

To improve the ability of allied governments to identify and report imminent CBRN attacks, NATO's Standardization Office publishes an operators' manual, "Warning and Reporting and Hazard Prediction of Chemical, Biological, Radiological and Nuclear Incidents," which is periodically updated.[31] NATO members have also adopted CBRN warning and reporting software to support the implementation of CBRN tactics and doctrine, and to improve the communication of critical information during a CBRN event.[32]

The Joint CBRN Center of Excellence (COE), based in the Czech Republic, has played a major role in embedding CBRN response in NATO doctrine and planning. The COE

NATO Drives the Sharing of Information and Awareness: The ISAF Afghan Mission Network

NATO's adoption of CBRN capabilities provides just one example of the ability of the alliance to adapt to new challenges and operational environments. In a separate instance, NATO mustered cyberspace capabilities to successfully improve theater communications and information sharing in the midst of coalition operations in Afghanistan. Between 2008 and 2010, the ISAF Afghan Mission Network (AMN) moved from a proposal to an operational concept through a mandate that coalition nations share information and command, control, communications, computers, combat systems, intelligence, surveillance, and reconnaissance (C5ISR) on a single information infrastructure. As a result, at the highwater mark in 2011, 48 NATO and partner states were operating on AMN. The network was built through successful incremental steps, such as securely connecting the NATO secret network (NATO General Purpose Communications Systems/NATO Secret) to trusted nodes in the wider coalition secret network (ISAF-Secret).

To achieve this, the AMN "field expedient mindset" supported unity of effort through shared information and awareness. The initiative provides an exemplary model for the NATO day-to-day network across Headquarters, alliance business, and deployed forces. With the AMN approach, policies, governance, and protocols will be in place for NATO's "mission network" and can be adjusted to ongoing gap analysis and to absorb new capabilities and partners.

In a 2014 assessment of the AMN, RAND analysts concluded that "NATO, the UN, and U.S. Combatant Commands (CCMDs) beyond USCENTCOM witnessed the value and potential of coalition networking. Lessons were learned that hopefully will not have to be relearned in future efforts. . . . AMN not only yields important lessons in this regard, it also serves as an experiential reference point that will likely shape future efforts, understandings, and expectations."*

Future architecture for such a network could apply contemporary designs for coalition information-sharing, such as a hybrid government and commercially provided cloud service as the foundation of a network to share all coalition information. This approach would allow a new coalition subnetwork to be established quickly at the assembly of a new coalition mission or exercise. New instances of partner networks can be spun at operational headquarters to offer partners the ability to connect with their own devices and hardware and can be decommissioned when no longer needed. At the tactical edge, mobile devices can access the data necessary to share information and awareness.

AMN provides an example of NATO's ability to field an important new mission capability, delivered in part by technology. More importantly, it is an example of alliance military leadership in driving change through a commitment and capability to share information necessary for mission effectiveness.

* Chad C. Serena, Isaac R. Porche III, Joel B. Predd, Jan Osburg, and Brad Lossing, *Lessons Learned from the Afghan Mission Network*, Santa Monica, Calif.: RAND Corporation, RR-302-A, 2014, p. 7.

actively supports ACT in the identification of minimum capability requirements for NDPP.[33] In addition to NDPP support, COE's Transformation Support Department also supports the development of NATO doctrine: An Allied Joint Doctrine for CRBN, published in 2012 and updated in 2018, provides doctrinal guidance for alliance CBRN operations.[34] Through the COE, NATO is able to provide continuing support at the national level for CBRN concept, doctrine, procedures, and standards development for individual NATO member states and partners.[35] The COE also helps to ensure that doctrine is translated into operational skills and knowledge: CBRN Warning and Reporting Specialist Courses, initiated by the COE in 2012, trained groups of military officers from across the alliance in the NATO operations manual, procedures, and software associated with CBRN warning and reporting.[36]

Conclusion

While the introduction of cyberspace as an operational domain may present new institutional challenges for NATO, there is certainly precedent for alliance evolution. NATO's development of responses to CBRN threats offers one such example and provides insights for future NATO cyberspace initiatives. Specifically, NATO successfully established a robust exercise and training program to hone and improve the initial CRBN response concept. Through exercises and training—and by leveraging niche areas of expertise within the alliance—NATO has made strides in overcoming gaps in knowledge and skills within individual member states, and more could be done to extend exercises to further incorporate civilian entities. Efforts to embed NATO's CBRN initiatives into doctrine, planning, and prediction at both the alliance and national levels has helped to ensure that CBRN capabilities would be operationally relevant during a conflict. However, sustained effort is required to ensure allies prioritize the resources and capabilities required to contribute to a collective CBRN defense.[37]

It should be noted, however, that there are at least two important differences between CBRN and cyber. First, cyber is clearly a nongeographical domain, which requires a shift of understanding for commanders. Second, cyber is a highly technical domain, where industry is considerably more prepared than military organizations, and, therefore, commanders must learn to adapt with industry as a strategic mission partner.

NATO's Present: Operationalizing Cyberspace Across the Alliance

Since the June 2016 NATO ministerial recognized cyberspace as an operational domain, the alliance has approved a cyberspace roadmap; announced the establishment of a new Cyberspace Operations Center (CyOC); established new staff functions at its two strategic commands; and agreed to a military vision and strategy for cyberspace operations.[38] These important steps are indicative of the challenges facing NATO, especially given the breadth of the alliance, the relative immaturity of the cyber domain, and the variability in allied capabilities and experience in cyberspace.

From the cyberspace roadmap to the CyOC, a number of building blocks are preparing NATO to operate effectively in the cyber domain. This effort is ambitious and will require concerted focus and integration across the 29 allies and NATO. Evaluating the degree of alignment between national-level approaches and NATO's publicly stated priorities and goals can indicate where allies are pursuing national efforts that support the full alliance.

RAND reviewed 80 open source documents to evaluate the degree to which national documents echo or support similar approaches to those of NATO. We performed topic analysis and identified five potential areas of convergence or divergence. The documents included national security strategies and defense white papers; national cyber strategies and action plans; critical infrastructure strategies and action plans; and legislative acts, executive orders, and other relevant documents. Originating entities included, but were not limited to, defense ministries, intelligence agencies, interior ministries, the executive branch, the legislative branch, multi-agency/whole-of-government entities, independent cyber authorities, and other entities with law enforcement functions. The analysis found general agreement across NATO allies in several important areas.

First, NATO has publicly identified "cyber defence [as] part of NATO's core task of collective defence."[39] The majority (50 out of 80) of the documents described strengthening national cyber defense as an official objective. Documentation addressed increased resiliency for both civilian and government cyber infrastructure, and roughly a quarter of documents discussed further developing cyber defense capabilities in a military context.

Secondly, NATO has called for "developing the NATO cyber defence capability" and "increasing NATO cyber defence capacity."[40] Most national strategies, plans, and white papers emphasized the importance of building cyber capabilities in both the public and private sectors. Three-quarters of allied nations produced documentation that called for building cyber capacity and capabilities. However, fewer than half of member states published strategies that called for cyber defense-specific improvements. This is particularly concerning given that defense (whether in cyber or any other domain) requires maturity from all participants and is therefore only as reliable as the weakest protection measure.

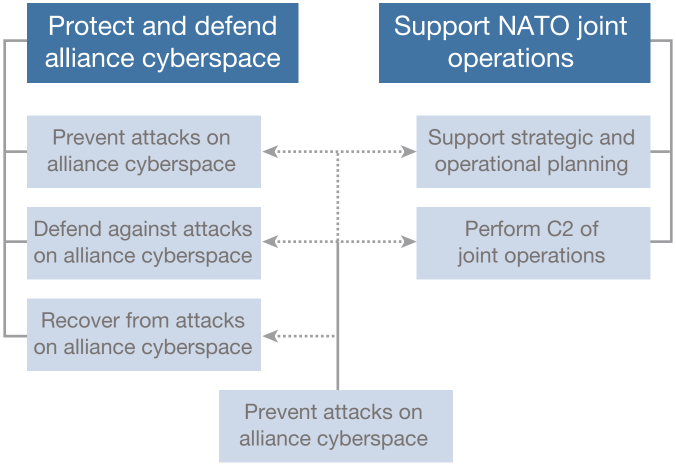
Finally, NATO has also emphasized the importance of cooperation with partners and industry: "Because cyber threats defy state borders and organisational boundaries, NATO engages with relevant countries and organisations to enhance international security;" and "The private sector is a key player in cyberspace, and technological innovations and expertise from the private sector are crucial to enable NATO and Allied countries to mount an effective cyber defence."[41] NATO allies' cyber strategies, action plans, and white papers overwhelmingly supported and reflected this approach. Every NATO member state—as evidenced in more than three-quarters of the documents RAND reviewed—highlighted the importance of international cyber cooperation, whether via NATO, the European Union (EU), Computer Emergency Response Team (CERT)-to-CERT collaboration and information sharing, or other means. Similarly, every NATO member state—as evidenced across nearly three-quarters of documents—highlighted the importance of building and sustaining public-private partnerships.

Implementing changes will require a cultural shift across the alliance, as well as changes to policies, processes, procedures, capabilities, training, education, exercises, and planning, as well as appropriate metrics by which to measure and evaluate each of these steps. In this section, we highlight several initiatives that are of primary importance to ensure that NATO is successful in adapting itself to succeed in cyberspace: defining cyberspace functions to operationalize the domain; exercises and training to develop competency, including the supporting infrastructure; and developing the cyber workforce.

Cyberspace Functions

For NATO to defend itself in cyberspace, it must develop the capacity to prevent attacks on alliance cyberspace, defend against ongoing attacks, and recover from attacks that break through NATO defenses. Cyberattacks can come in many forms, from nuisance attacks that might result in defacement of public-facing websites to much more sophisticated attacks that prevent NATO from conducting its missions or leading to loss of life or destruction of property. Integrating cyberspace into NATO operations requires supporting strategic and operational planning and performing command and control of cyber forces in the context of joint operations. Underpinning both strategic ends is the need to develop and maintain situational awareness of cyberspace, whether it is knowing the operating status of NATO networks or developing early warning of potential adversary cyberactivity. These functional areas are reflected in Figure 1.[42]

FIGURE 1
NATO Operational View


Protect and defend alliance cyberspace
Support NATO joint operations
Prevent attacks on alliance cyberspace
Support strategic and operational planning
Defend against attacks on alliance cyberspace
Perform C2 of joint operations
Recover from attacks on alliance cyberspace
Prevent attacks on alliance cyberspace

NOTES: C2 = command and control. We define attack as a compromise of alliance systems' confidentiality, availability, or integrity. Note that by protecting and defending alliance cyberspace and by supporting NATO operations, NATO will also be able to maintain deterrence options.

These are high-level descriptions of the major functions NATO has to carry out to operate and defend in cyberspace. Whether NATO as an alliance has the requisite capabilities to perform these functions is an ongoing area of analysis, but it is likely that NATO will discover areas requiring further development and acquisition. For example, NATO defines situational awareness as “knowledge of the elements in the battlespace necessary to make well-informed decisions.”[43] Defining the battlespace for cyberspace is uniquely challenging, though it encompasses such traditional military concepts as understanding adversary activities and capabilities as well as allied activities and capabilities. Cyberspace as a topic of discourse is rife with competing lexicons, concepts, and terms that NATO is currently working to clarify, not only in its terminology, but also through implementing common standards for information exchange.

More broadly, defense of the alliance in cyberspace encompasses first defining what threats the alliance must be prepared to face and where it can act to defend itself, then ensuring that the capabilities and capacity are available to successfully defend itself. Since the end of the Cold

War, NATO has expanded its reach both in terms of membership and partners and in terms of its operations. As a globally engaged organization, NATO must be prepared for addressing cyber threats that emanate from anywhere in the world. In cybersecurity, situational awareness often focuses on maintaining persistent insight into the functioning and health of one's own networks.[44] For NATO, however, this is complicated by the federated nature of the alliance, where individual states are responsible for their own networks, but attacks that manifest in one area could easily spread to others, whether from NATO networks to a nation's or vice versa. The question becomes how NATO maintains insight into what is occurring beyond its own networks, particularly when nations are connected together in an operational context. Will NATO receive information on the status of U.S. or Hungarian military networks, for example, or will NATO monitor only its own networks, up to some ill-defined boundary where states connect? Strong capabilities with I&W, for example, can greatly help and are discussed more in the following section. To start, however, NATO needs to implement and maintain a common baseline of minimum cybersecurity standards and actions across the alliance and all members. This should include establishing and tracking metrics to facilitate a common understanding of NATO's cybersecurity posture.

Integrating cyber operations into NATO's existing processes and procedures for planning and conducting joint operations is more than a matter of simply developing annexes in plans or adding cyber planners at SHAPE headquarters, though this is an important part of the process for operationalizing cyberspace. To truly integrate cyber operations requires broadly educating the alliance on operations in cyberspace, training and exercising to create the "muscle memory" necessary, and rigorously assessing lessons learned as they emerge. The disparity in cyber capabilities across the alliance, as well as the highly classified nature of some of the allies' capabilities, makes this more difficult (but not impossible) to achieve.

NATO has an extensive array of doctrine and policies to guide operations, including existing policies on cybersecurity and defense, but less focus on the integration of cyber operations into joint operations currently.[45] NATO's *Comprehensive Operational Planning Directive* (COPD), for example, provides detailed guidance on how to conduct planning at the operational and strategic levels, and the most recent interim version from 2013 references cyber defense in a few places. This is not entirely surprising, given the age of the document. As a general guide to operational planning, the COPD in itself is flexible enough to accommodate integration of cyber operations with minor changes (such as including explicit references to cyber effects matrices or similar tools for planning considerations). NATO is developing doctrine for cyber operations as well, which will evolve over time as the alliance gains experience.

Then–U.S. Secretary of Defense James Mattis committed at the October 2018 Defense Ministerial to support NATO with U.S. cyber capabilities but did not publicly provide further details.[46] NATO has a defense planning process intended to identify and ensure that capabilities are available to meet NATO needs in the medium to long term.[47] Given the sensitive nature of some nations' cyber capabilities, it may prove challenging for NATO, as a whole, to truly understand what capabilities are available to it and whether and how to fill the gaps that exist. This clearly is a challenge on the offensive side, which

NATO will look entirely to member nations to maintain, but also could apply to higher-end defensive capabilities, particularly those derived from intelligence sources. NATO operational planners will therefore have to adapt to planning under conditions of uncertainty, seeking to plan for effects and capabilities into which they do not have full insight. Overcoming these challenges will take time and can be mitigated through a strong exercise program. Now, this situation is no different from any other domains where nations provide forces and weapons, and NATO provides joint C2. A key difference in cyber, however, is that nations are not yet ready to disclose their offensive capabilities as readily as they do in other domains, which complicates planning, executions, and assessments.

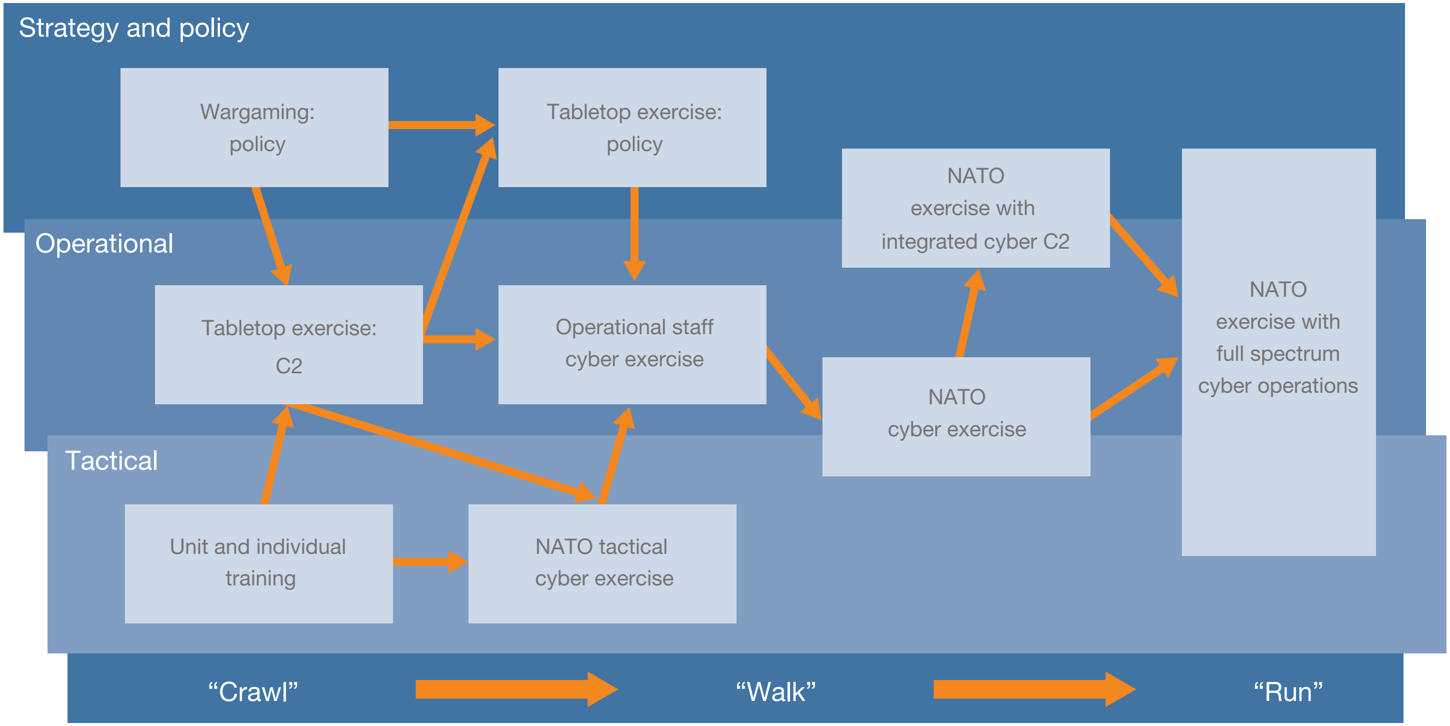
Exercises and Training

In October and November 2018, NATO conducted Exercise TRIDENT JUNCTURE in Norway, one of its largest field exercises in recent history.[48] Secretary General Jens Stoltenberg noted that the exercise tested the alliance's ability to engage in collective defense, not only on land, sea, and in the air, but also in cyberspace.[49] This exercise is an important element in integrating cyberspace into NATO operations; however, the public reporting gives little insight into how much cyberspace played a role in affecting other domains of warfare in the exercise. NATO's main cyber defense exercise, Cyber Endeavor, took place after TRIDENT JUNCTURE in late November, which indicates it was not closely tied to operational field exercises.[50] NATO will have to address developing capacity at multiple levels, from the lowest tactical level to the strategic, for cyber defense and integrating cyber into joint operations through a tiered, progressive approach to exercises.

Military cyber exercises present challenges in realism and in developing the knowledge, skills, and procedures necessary for successful integration into overall operations. One can categorize exercises involving cyber operations into three main types covering the full spectrum of cyber operations or portions thereof: strategy and policy, operational integration, and technical application, as shown in Figure 2.

Exercising strategy and policy typically occurs during senior leader staff exercises or tabletop exercises. This focus on higher-level strategy and policy issues allows for consolidating timelines and covering more topics without the distraction of integrating live forces, which can quickly dominate an exercise. The purpose of these kinds of exercises is to identify challenges, develop familiarity with concepts at the strategic and operational levels, and inform updates to doctrine, policy, and planning guidance. Last year's Exercise Cyber Coalition would appear to be the equivalent of a cyber exercise at the operational and tactical level, since it was not apparently tied into noncyber exercises. Cyber Coalition's scenario focused on, among other things, protecting elections and other critical infrastructure from attack, whereas TRIDENT JUNCTURE focused on field exercises to defend NATO territory from conventional attack. This does not mean the exercises are not important steps, and in fact they demonstrate that NATO is in some respects already in the "Walk" phase of an exercise plan. NATO will undoubtedly find, however, that it needs to return to earlier phases as new staff rotate in and the alliance evolves its understanding of the threat environment and its own capabilities.

FIGURE 2
Example Exercise Plan


Strategy and policy
Wargaming: policy
Tabletop exercise: policy
NATO exercise with integrated cyber C2
NATO exercise with full spectrum cyber operations
Operational
Tabletop exercise: C2
Operational staff cyber exercise
NATO cyber exercise
Tactical
Unit and individual training
NATO tactical cyber exercise
"Crawl"
"Walk"
"Run"

Integrating cyber into joint operational processes is crucial. A first step is to recognize organizational changes and how those organizations plan and execute with traditional forces. The next step is to integrate cyber into the battle rhythm of headquarters' staff at various echelons. Some aspects of cyberspace operations are not unique, such as using the operational planning process for effects-based planning. Other aspects are distinct, such as authorities to execute cyber operations. Understanding these differences is the key to operationalizing cyber. Operational-level exercise events should result in updated operational planning and execution processes, and staff that is better prepared to plan for, execute, and evaluate cyberspace operations.

The tactical application of cyber is typically more straightforward than at the operational, strategy, and policy levels because it is bounded by technology and can focus on concrete tactics, techniques, and procedures (TTPs). Exercises in this area will typically focus on network operations and defense but could extend to include the integration of electronic warfare platforms and live targets, or developing and implementing indicators for cyber threat warning, as we will discuss in more depth in the next section. Defensive operations often require an exercise range so as to not impact real world operations or compromise live networks.

Given that NATO is not going to conduct offensive cyber operations itself (though it may integrate effects from allied nations), it will still need to use exercises to account for how it requests national-level effects and integrates them into planning.[51] This is best addressed in an operational-level exercise but could extend to a technical level by having effects represented in some fashion on a NATO cyber range, to provide context to which other players respond. These cyber ranges are particularly useful, since employing these capabilities on a live network can lead to adverse outcomes, such as destruction of real data or loss of system functionality.

Exercising defensive cyber operations is trickier. Part of the exercise should be conducted by a red team on real defended networks. This allows for penetration testing of the networks and exercising defensive forces in the most realistic environment possible. However, part of the exercise must also occur in a simulated environment (i.e., a cyber range) to mitigate risks to real networks and allow for more dynamic interaction between network defenders and attackers. This approach often sacrifices some level of realism, but that is unavoidable given the risks to real networks and the challenges in providing a true emulation of large, complex networks such as NATO's Communication and Information System (CIS) network.

NATO concluded an agreement with the Estonian government in 2014 to leverage its national cyber range for NATO use.[52] Determining whether this range architecture is sufficient for all of NATO's needs will first depend on conducting a needs assessment and capability gap analysis. It is reasonable to conclude that NATO's exercise and training regimen for cyberspace will grow in the coming years, which would indicate a need for more capacity and certainly a need for greater range capability to adapt to changing technology.

NATO could supplement the Estonian capabilities with commercially available cyber ranges, which often employ cloud architecture. The advantage of using a full-service vendor instead of a generic cloud service provider (e.g., Amazon Web Services, Google Cloud) is that it can easily generate network traffic and replicate cyberattacks. These vendors also provide all the range infrastructure, allowing the students to merely "plug and play." Using a cloud service provider would require that NATO have the staff expertise to develop and maintain the range specifications and vignettes; set up and manage the range during an exercise; and capture exercise data for subsequent improvement to the range instantiation. A commercial vendor that offers a "range as a service" would handle these aspects in a way that a cloud vendor would not (or would be potentially willing but ill-suited to do).

The training and equipping of military forces are a national responsibility, and states are also responsible for validating and passing fit cyber units that contribute to NATO missions (what is referred to as force certification). The primary purpose of a NATO cyber range infrastructure would be to support combined joint exercises of national cyber units reflecting how they will operate under a NATO command infrastructure. Many states will operate their own range infrastructure for national purposes, such as training and exercising to national objectives—including multidomain operations, developmental and operational tests, and experimentation. NATO may choose to provide range access to states for this purpose if they do not have their own range or are in the process of establishing one.

The integration of cyber effects into military operations to operationalize the domain fully is an ongoing process at the national level, just as it is an area of development for NATO. The United States, for example, has experimented with multiple approaches to develop planning processes and personnel to integrate with operational staffs—including liaison officers from its Cyber Command to the geographic and other functional combatant commands and creating Joint Cyber Centers across the headquarters staffs to combine intelligence, operations, planning, and communications—but these approaches are still evolving. In addition, the authorities to execute cyber operations, while often focused on offensive action, are also an ongoing discussion in defensive operations. This is where a series of high-level strategy and operational tabletop exercises can inform NATO how best to identify the key issues, experiment with alternative constructs, and evaluate the most useful approach that works for the alliance.

Workforce

NATO will need staff officers, civilian personnel, and other augmentees who not only are steeped in the technical aspects of cyberspace but also understand how cyberspace operations can contribute to the overall success of NATO operations and how other domains can reinforce the cyber domain. NATO is starting to adapt its educational curriculum to address the full array of cyberspace issues. The NATO Communications and Information Agency has built a new school in Portugal to support its mission and teach staff about the operation of NATO IT systems.[53] Other academic institutions, such as the NATO Defence College, the NATO School Oberammergau, or the Cooperative Cyber Defence Centre of Excellence, should also implement courses focusing on cyberspace as a domain of operations.

> The competition for skilled cybersecurity personnel is well documented.

The competition for skilled cybersecurity personnel is well documented. The cybersecurity certification organization, (ISC)^2, noted in a recent report that the workforce shortage of these professionals is growing globally, reaching almost three million positions in 2018.[54] Nearly half of the surveyed organizations for that report expected to increase cybersecurity staffing in the next year, underscoring that demand will grow, not diminish. NATO undoubtedly will be among those organizations competing in the labor marketplace for skilled cybersecurity professionals, but as we have seen, it will require more than technical staff. It will need to educate its leadership, both military and civilian, in the technical, operational, legal, and policy topics of cyberspace.

Officers and civilian personnel assigned to NATO on rotations will come with varied backgrounds and

NATO will need to address how it recruits and retains personnel to identify opportunities for attracting talent and taking advantage of expertise.

experience for the positions they will fill. Some positions, such as in the cyber offices at Allied Command Operations (ACO), ACT, and the new CyOC will clearly need personnel who have a deeper experience than the broader organization, something that will likely rely on personnel from a subset of the member nations for the near future, given the wide variance in national experience in cyberspace. But other parts of NATO will also need to draw on cyber expertise to ensure cyberspace integration into operations, including at the various operational headquarters.

A first step to ensuring that qualified personnel are assigned (part of which has already been completed by the NATO Command Structure Adaptation that reviewed, among others, ACT and ACO cyber positions) is to evaluate and enumerate the specific job functions and associated qualifications for cyber-related positions across the alliance. These can include planners, operators, cyber defenders, acquisition personnel, and even less-obvious areas such as public diplomacy.

NATO relies on its member nations to send qualified personnel on rotation, but NATO also has longer-serving staff among its civilian personnel. Whether employees have served for three years or 30, NATO will want to ensure that its cyber workforce has a baseline of skills and knowledge and develop progressive educational modules to grow and sustain its human capital. As already noted, the baseline will vary depending on the work roles and job series a person occupies. The U.S. Department of Defense (DoD) has developed a DoD Cyber Workforce Framework that encompasses four main categories of personnel: cyberspace IT, cybersecurity, cyberspace effects, and intelligence.[55] NATO could also look to bring in expertise on short-term assignments similar to the U.S. Defense Digital Service.[56] It could also develop industry fellows programs to give its permanent staff experience in the private sector, similar to the U.S. Secretary of Defense Executive Fellows program.[57] These programs could inject new thinking and bring valuable private-sector experience to bear.

NATO's educational institutions will play a critical role in developing and sustaining the cyberspace workforce for the alliance, starting with instituting courses that cover relevant topics, from strategy and policy to more technical areas. Some suggested topics to include in a first orientation course that establishes the baseline (some of which are already being taught) would include

- NATO *organizational structure* and national-level organizations that interface with the alliance. This would include covering the roles and responsibilities of the NCIRC, ACO Cyber Division, ACT Cyber Capabilities Branch, and the CyOC, as well as national-level cybercommands and EU institutions.

- *strategic and operational planning*, including how cyber operations fit into the COPD and the NATO Crisis Management Process.
- *technical topics* for those less familiar with the layers of the cyber domain, from the physical infrastructure to the virtual or "cyber persona" domain.
- *cyberspace capabilities* in the alliance and at the national level, including defensive capabilities.
- the *legal and policy* frameworks for cyber operations, including the law of armed conflict and its application to the cyber domain, operational authorities, and NATO declarations and policies.

Finally, NATO will need to address how it recruits and retains personnel to identify opportunities for attracting talent and taking advantage of expertise. Initiatives could include offering limited-term appointments from the private sector, scholarship-for-service, and developing stronger ties with academic institutions across the alliance.

Conclusion

For NATO to achieve the ambitious goals it has set for itself in Ministerial statements, it will take sustained effort and dedication. Each member has a role to play, at the very least in shoring up its own cyber defenses, as well as contributing to the extent it can and is fit for purpose to the overall defense of the alliance. In this section, we highlighted key areas to focus on in terms of defining cyberspace functions, exercises and training, and workforce development, but as is often the case, there are numerous other areas requiring focus. Numerous members large and small have clear capabilities in cyberspace. Harnessing those capabilities in an integrated manner will not happen overnight, but NATO has the capacity and mechanisms to accomplish its goals.

Preparing for the Future: Indications and Warning Against Cyber Threats to NATO

Why I&W Against Cyber Threats?

Effective and timely I&W of cyber threats is a vital component of any cyber strategy because they can provide early detection and advance notification of cyber threats. This early warning can facilitate avoidance or mitigation of potentially harmful attacks by providing decisionmakers with needed time to consider options and authorize and implement preventive actions. Yet none of the cyber strategies released by the United States or its federal agencies discuss I&W in detail. National cyber strategies of other NATO members likewise do not elaborate on I&W of cyber threats, likely due to the lack of clearly established definitions or best practices on how to construct I&W frameworks in the cyber domain. The need to constantly refine and adapt these frameworks to the evolving threat actors provides further challenges for establishing a standardized cyber I&W model.

It is specifically *because* of these challenges that it becomes critical to identify the main parameters of an effective cyber I&W framework. For example, cyber I&W will help to ensure robust defense of the alliance's cyberspace and continuous operation of NATO's cyber infrastructure in support of strategic and operational planning. I&W capabilities for the cyber domain are also directly related to the functional areas of NATO's operational view

Cyber I&W focuses on collecting actionable information about threats to cyberspace that may provide early detection and warning of impending malicious cyberactivity.

as described in Figure 1. To be effective at predicting and detecting threats to cyberspace, I&W frameworks require both horizontal (NATO-wide and across NATO members) and vertical (within NATO entities, nations, and sectors) integration and collaboration, including national contributions and collaboration between nation-states and national entities at multiple levels. Thus, designing rigorous I&W frameworks in cyberspace is a complex challenge that requires a number of key steps: crafting a strategy for cooperation and communication among NATO entities, NATO members and partners, and other public-private entities; developing information-sharing protocols that ensure timely and continuous data exchange; and integrating I&W cyber frameworks in joint cyber exercises to improve I&W applications.

Despite the significance of the field and some promising steps toward improving cyber I&W capabilities, frameworks for cyber I&W are still evolving and are not yet mature.[58] The importance of I&W methods, combined with their relatively recent and underdeveloped application to cyberspace, suggests this issue warrants special attention.

In their process of designing a robust and adaptable cyber I&W framework, NATO entities may benefit from understanding how mature I&W frameworks from other domains in U.S. intelligence can be adapted to the cyber domain. Such I&W frameworks offer a way of thinking about security threats and provide methods for designing and structuring detection and response mechanisms.

In this section, we first define I&W, and then outline the publicly known progress that NATO has already achieved in relation to building its cyber I&W capabilities. We then propose a general framework for cyber I&W and discuss how NATO can further develop, adopt, and integrate cyber I&W capabilities within its current planning processes and operations. We conclude with an overview of several critical issues that we believe NATO entities should address to ensure that the alliance meets its mission-critical objectives in cyberspace.

What Is Cyber Indications and Warning?

Cyber I&W focuses on collecting actionable information about threats to cyberspace that may provide early detection and warning of impending malicious cyberactivity. However, there is still no consensus regarding the concept of *indications and warning*. Some liken it to cyber threat intelligence and therefore focus on information directly pertaining to impending threats without analyzing broader strategic-level factors that can affect the behavior of a threat. Others define cyber I&W as a methodology that includes monitoring for indications of an impending threat, understanding the context in which this information is being collected, and performing strategic-level assessments of these indicators that can affect the behavior or nature of an impending cyberattack.[59]

Publicly available U.S. doctrine offers some insights applicable to the NATO context that can serve as a starting point for discussion. U.S. Joint Publication 2.0 stipulates that *warning intelligence*—a concept the DoD has recently adopted instead of *indications and warning*—includes "those intelligence activities intended to detect and report time-sensitive intelligence information on foreign developments that forewarn of hostile actions or intention."[60] Joint Publication 3-12 further stipulates that warning intelligence should be based on "all-source analysis in order to factor in political, military, and technical warning intelligence" and that "cyberspace threat sensors may recognize malicious activity with only a very short time available to respond."[61] While these definitions characterize the nature of cyber I&W concepts, they do not provide a full explanation of how to design an I&W framework.

The term *indications and warning* has a formal meaning in NATO and is supported through a set of processes governed by the member states with strong involvement by their intelligence communities.[62] Yet NATO does not publicly offer a formal definition of what constitutes I&W in the cyber domain. Official public NATO documents provide only some insights; for instance, NATO's *2018 Glossary of Terms and Definitions* defines *strategic warning* as "[a] notification that hostilities may be imminent. This notification may occur at any time prior to the initiation of hostilities." The document also defines *tactical warning* as "[a] notification that a local enemy attack is imminent. This notification may occur at any time from the indication of a probable attack until just prior to the target being struck or engaged."[63] The glossary defines *indicator* as "an item of information which reflects the intention or capability of a potential enemy to adopt or reject a course of action."[64] Although informative, these definitions provide only a general understanding of what activities constitute I&W. One distinction that can be made is separately defining indications from warnings. One may consider that there are indicators at various levels: strategic indicators (usually based on intelligence); operational indicators (combining intelligence and technical information); and tactical indicators (technical intrusion—malware, phishing, etc.). Warnings describe how and when to relay the indicators to the field.

Finally, the Intelligence and National Security Alliance (INSA), a U.S.-based nonprofit organization that facilitates collaboration between the private and public sectors concerning national security and intelligence,[65] defines I&W against cyber threats as "an analytic process where an anticipated scenario in cyberspace is decomposed into indicators that can be continuously monitored to provide warning of the scenario coming to fruition."[66] We propose to adapt this definition to the NATO context and emphasize NATO's primary area of responsibility and the political utility of I&W frameworks. We therefore define I&W for cyber threats as "an analytical process focused on collecting and analyzing information from a broad array of sources to develop indicators which can facilitate the prediction, early detection, and warning of cyber incidents relative to one's information environment."[67] These indicators are then continuously monitored to provide warning of the scenario coming to fruition as much in advance as possible, allowing NATO to take preventive action.

Before we outline our framework, we first describe how NATO has already prepared its infrastructure for addressing, at least in part, cyber I&W.

How Has NATO Already Prepared for Cyber I&W?

NATO has made significant progress in elevating the importance of the cyber domain and setting up the structural foundations for the effective adoption and integration of cyber I&W frameworks. In particular,

- At the Wales Summit in September 2014, NATO adopted an action plan for enhancing cyber defense, which was subsequently updated in February 2017.[68]
- At the Warsaw Summit in 2016, NATO members agreed to prioritize the strengthening of the cyber defenses of their national infrastructure and networks.[69]
- At the Brussels 2018 summit, NATO members discussed collaboration between NATO entities and nation-level cyber capabilities and teams. In the Brussels Summit Declaration, issued by NATO's heads of state and government, the allies asserted that NATO "will continue to optimise NATO intelligence to facilitate timely and relevant support to Allied decision-making and operations, including through improved warning and intelligence sharing, particularly on terrorism, hybrid, and cyber."[70]
- NATO claims to continuously update its cyber policy and its action plan, which contains "concrete objectives and implementation timelines on a range of topics from capability development, education, training and exercises, and partnerships" to include, for example, allied nations agreeing to a Cyber Defense Pledge to prioritize maturing their security controls.[71]

NATO has made significant progress in standing up NATO entities and capabilities to implement or be involved in the implementation of I&W frameworks for cyber threats. Some of the principal NATO organizations include

- *NCIRC,* operated by NCIA and based at SHAPE in Mons, Belgium, is responsible for protecting NATO's networks. NCIRC monitors, prevents, detects, and responds to cybersecurity incidents and provides centralized cyber defense support to NATO sites.[72] In 2006, NCIRC obtained its initial operating capability and started to build more robust cyber situational awareness for NATO's networks. In 2013, NCIRC expanded its intrusion detection monitoring capabilities to more NATO critical sites under the Full Operating Capability program. The sites were expanded again in 2017.[73]
- *NATO's CyOC*, established at the Brussels Summit in 2018 as a part of NATO's Command Structure and located at SHAPE. Among other responsibilities, the CyOC acts as a focal point for planning, preparation, conduct, and coordination of cyberspace operations, which will involve the processing and analysis of data.[74] The CyOC is established to support I&W decisions, though it does not maintain a separate cyberspace I&W framework.[75]
- *ACO Task Force Cyber* is a multidisciplinary team acting as a part of Supreme Allied Commander Europe's task to provide the Council with advice on I&W on threats to NATO's collective security.[76]

- *ACT* is NATO’s warfare development command and capability requirements authority, responsible for NATO common funded capability delivery.
- *NATO’s Intelligence and Security Division*, supported by SHAPE Comprehensive Crisis and Operations Management Centre, NATO Intelligence Fusion Centre, and the national representatives, is responsible for the NATO I&W System, which incorporates I&W capabilities in cyberspace.[77]
- *NATO Intelligence Fusion Centre*, a multinational organization operating under a memorandum of understanding (MOU) with SHAPE, provides the primary intelligence analytical support.[78]

NATO’s educational structures have also substantially evolved and expanded their cyber education and training. NATO’s principal educational institutions include

- the *NATO Cooperative Cyber Defence Centre of Excellence* (CCDCOE) in Tallinn, Estonia, a NATO-accredited research and training center providing education, consultation, research, and development in the area of cybersecurity
- the *NATO Communications and Information Systems School* in Latina, Italy, which provides training on operating and maintaining NATO’s communication and information systems to personnel from NATO members and allied nations[79]
- the *NATO School* in Oberammergau, Germany, which provides cyber defense education and training in support of NATO operations, policy, doctrine, strategy, and procedures

NATO entities and allies have also recognized the importance of partnering with the private sector.

- the *NATO Defense College* in Rome, Italy, which emphasizes strategic education on cyber defense issues.[80]

NATO entities and allies have also recognized the importance of partnering with the private sector. Some of the benefits of such cooperation include establishing sharing of best practices and lessons learned and ensuring the timely supply and analysis of actionable cyber threat information. One of the primary channels through which NATO strengthens its collaboration with private partners is the NATO Industry Cyber Partnership. The partnership includes NATO structures, national CERTs, and industry representatives of NATO members. The partnerships include information-sharing activities, training, exercises, and multinational Smart Defence[81] projects.[82]

Adopting Strategic Intelligence Frameworks to Cyberspace in the NATO Context

Despite significant progress in building cyber capabilities and integrating them into existing NATO planning, operations, and C2 structures, I&W for cyberspace is still a relatively immature discipline. Therefore, NATO and its components can benefit by adopting well-established and tested frameworks from more mature disciplines, which provide actionable policy-relevant recommendations related to the detection and assessment of security threats. For instance, cyber I&W concepts can leverage the I&W frameworks used by U.S. strategic intelligence, the Department of Homeland Security, or Cyber Command. The U.S. intelligence community has been developing and improving these frameworks since World War II to assess and monitor potentially threatening actions by U.S. adversaries in an attempt to avoid surprise attacks, such as the attack against Pearl Harbor in 1941.[83]

Among the most well-known warning intelligence frameworks are former senior intelligence analyst Cynthia Grabo's comprehensive methodology for warning intelligence, Jonathan Lockwood's Analytical Method for Prediction, and the U.S. Defense Warning Network conceptual framework.[84] However, the cyber I&W framework produced by INSA reflects components of these traditional I&W intelligence frameworks and provides an appropriate model that can be adapted to the NATO context.[85] INSA's framework is a useful starting point for building a cyber I&W foundation because it was based on tradecraft from the U.S. intelligence community in consultation with governmental, academic, and private sector representatives and is one of the only publicly available documents on this topic. INSA's original I&W framework contains the following seven steps: (1) identify and prioritize assets, (2) refine the threat, (3) assess threat courses of action, (4) break down scenarios into indicators, (5) plan and exercise countermeasures, (6) align to the intelligence cycle (collect information for each indicator from Step 4), and (7) execute proactive countermeasures.

While this framework is valuable and fills a gaping void for publicly available information on cyber I&W, its steps are too broad for our purposes. Therefore, we will adapt it to the NATO context and outline how NATO can apply these stages below. We closely adhere to the steps proposed by INSA but modify the sequence of Steps 5 and 6 to emphasize the need to establish data collection mechanisms for the indicators identified in Step 4 first, before planning and practicing countermeasures. In effect, one needs to be assured that the indicators are properly collected before responding to them.[86] We further discuss establishing standard operating procedures, exercising the planned countermeasures, and aligning them to NATO's communication and command structure in Step 6—this is necessary due to the tightly interconnected nature of these aspects of the process. For each step, we propose how NATO entities, allies, and partners can apply it to increase the effectiveness of their I&W capabilities by standardizing their operational protocols and decisionmaking processes. The RAND modified cyber I&W framework consists of the following steps:[87]

1. Identify and prioritize mission-critical assets.
2. Maintain an updated list of top cyber threats.
3. Construct scenarios of potential cyberattacks.
4. Decompose scenarios into observable indicators.
5. Establish data collection methods and sources and set up a collection requirement and prioritization matrix.
6. Establish standard operating procedures and exercise chain of communication and command in different scenarios.

Finally, it is important to recognize that some of the steps described below relate to common cybersecurity practices. However, the steps involving scenario development and identification of appropriate indicators are distinct and unique to a cyber I&W framework. This exercise is not meant to define a highly detailed framework but merely to highlight the key first steps the alliance should consider on its journey to operationalizing cyberspace.

Step 1: Identify and Prioritize Mission-Critical Assets

NATO's high visibility and central role in the Western security architecture make it an attractive target for a variety of malicious cyber intrusions.[88] The chief of cybersecurity at the NATO Communications and Information Agency (NCIA) asserts that NATO detects about 550 million suspicious events daily. Although NATO is constantly seeking to improve its cybersecurity, it is challenging to monitor, analyze, and act upon all of these events.[89] NATO's cyber I&W capabilities, therefore, must be able to differentiate between security alerts that represent a meaningful threat to the alliance (or are precursors to an attack) from activities that constitute operational noise that can be ignored.[90]

Suggested actions: To achieve this goal, NATO should leverage its mission assurance efforts to first determine a list of priority assets. The continued development of such a list should stem from NATO's primary mission to ensure collective defense and security of all its members, including the protection of communications systems that are owned and operated by the alliance.[91] NATO can further focus on supporting the protection of C2 nodes on NATO-based military sites that coordinate operations of major offensive military platforms, as well as telecommunications and electric grid systems, on which militaries heavily rely for intelligence, logistics, operations, and communications.[92]

Cyberspace is a highly interdependent domain with various central and peripheral information technology (IT) components, which, if compromised, can result in uncertain and cascading impacts to NATO's missions. Therefore, when establishing such a list of priorities, NATO entities should consider creating I&W prioritization tiers based on the criticality of NATO assets for mission assurance and whether those assets are located within or outside of NATO's theatre of operation. For example, the first I&W tier may focus on defending C2-critical systems within the theatre commander's control and operation. The second I&W tier can prioritize information assets outside of the theatre commander's control, and which have the potential to inflict the most damage on government IT, commercial providers, or critical national infrastructure networks.

Identifying and protecting critical infrastructure interdependencies in cyberspace against all seven of NATO's resilience baselines, such as communications, energy, and continuity of government services, should also be performed on a regular basis and in consultation with NATO member states and partner countries (at their request). The seminar on potential cascading impacts of disruptions in critical infrastructure sectors that took place in December 2018 at NATO's headquarters is an example of a practice that NATO could use as a platform for regular multi-stakeholder consultations on cybersecurity vulnerabilities in critical infrastructure.[93] The seminar gathered over 200 individuals from among NATO government representatives, the European Commission, academia, the private sector, and NATO partner countries.[94] NATO may consider holding such seminars annually and expanding their membership to ensure regular NATO-wide updates on emerging trends and exchange of best practices in the networks of its critical assets.

Step 2: Maintain an Updated List of Top Cyber Threats

In the second stage of constructing a robust I&W framework, NATO entities should use its existing threat assessment processes to identify a list of adversaries most likely to have capability, intent, and access, and which would potentially benefit from compromising NATO assets and missions. As NATO is primarily concerned with threats emanating from nation states, NATO's entities should focus on state-sponsored advanced persistent threat (APT) actors, particularly those that have already demonstrated a commitment to targeting NATO and multiple members (e.g., Russia's APT 28 [Fancy Bear] and APT 29 [Cozy Bear]).

Suggested actions: NATO member states and partners could establish regular meetings and create channels of communication to facilitate periodic consultations on top threat actors and, thus, modifications of NATO's cyber I&W framework.

Step 3: Construct Scenarios of Potential Cyberattacks

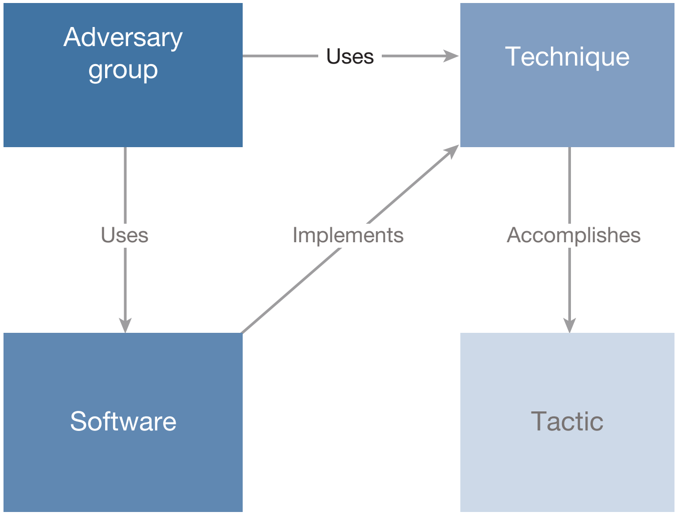
Once the main threat actors have been identified, NATO teams should construct scenarios of cyberattacks to derive indicators that will be used to detect imminent attacks. Here, NATO entities can benefit from existing analytical frameworks, such as Lockheed Martin's kill chain or MITRE's PRE-ATT&CK and ATT&CK frameworks, as shown in Figure 3.[95]

While ATT&CK and PRE-ATT&CK are perhaps most useful for threat analysts, red teams, or cyber defense teams responsible for NATO networks, the methodologies can be used for strategic purposes, as they provide a common lexicon that can be used to develop scenarios. A scenario-based approach is useful when considering all possible vectors of attack; however, this approach also has certain limitations. It is good only inasmuch as the defenders are able to conceive of all possible scenarios, collect data on all known previous attacks, and identify all possible indicators. As some past attacks are believed to have been conducted without being detected, and due to the constantly evolving TTPs of adversaries, it is likely the scenario-based approach will be able to anticipate only a portion of potential attacks on a given network.

Suggested actions: To ensure up-to-date threat assessment of its operational environment, NATO should continue to deepen cooperation with industry through NATO's Industry Cyber Partnership and through public-private partnerships.[96] Opportunities for cooperation include exchange of best practices and scenario development. Sharing of cyber threat indicators, data collection methods for different indicators, and information from analyzed cyber intrusions can facilitate deriving lessons learned and can improve existing detection and defense capabilities. NATO should similarly continue to strengthen cyber cooperation with the European Union and build upon the technical arrangement on cyber defense signed by both entities in February 2016.[97]

FIGURE 3

MITRE ATT&CK Model Relationships



SOURCE: Blake E. Strom, Andy Applebaum, Douglas P. Miller, Kathryn C. Nickels, Adam G. Pennington, and Cody B. Thomas, ***MITRE ATT&CK: Design and Philosophy***, MITRE Corporation, July 2018, Figure 2, p. 12. Used with permission.

Step 4: Decompose Scenarios into Observable Indicators

The scenarios discussed in Step 3 should be decomposed into observable indicators (e.g., behaviors or events, strategic, operational, or tactical), which can then be continuously monitored to identify a potential impending attack. Such indicators can include the names of domains used in C2 of attacks (tactical), email addresses used when registering the domains, email addresses used for spear phishing campaigns, and attachments infected with malware sent in spear phishing emails.[98] While the best indicators will be those that warn of an impending attack (strategic), the current state of the art in cyber I&W generally affords one the ability to identify only indicators from past attacks.

That being said, I&W collected from traditional intelligence channels can also provide valuable information on advance warning of cyber threats. A potential framework that can be applied to ensure a structured approach to incorporating all major domains from which indicators can originate is the *PMESII* model: political, military, economic, social, infrastructure, and information systems. Such a model would help categorize the data into logical compartments that enable comprehensive analysis of I&W data. It would ensure that the indicators used to monitor a certain cyber threat encompass not only technical developments but also geopolitical events that could signal a potential increase in malicious cyber capability or activity. For example, an increase in North Korea's cyber operations after announcements of a UN proposal for stricter sanctions against North Korea suggests a connection between these events.[99] Such knowledge can be used to formulate an economic indicator focused on monitoring the discussion of new sanctions against North Korea that can serve as one geopolitical predictor of North Korean cyberattacks. Such an indicator can be a part of the *economic* component of the PMESII model.

Another example of a potential *political* indicator that can serve to anticipate cyberattacks is national election cycles. Research by Comodo's Kenneth Geers shows an observed spike in malware detection before Turkey's 2018 elections, Russia's 2018 presidential elections, and in 13 swing states in the United States before the November 2018 midterm elections. The data show that such malware spikes start with reconnaissance via applications, followed by targeted malware distribution via worm and information

Besides being comprehensive, NATO's I&W framework should be flexible to accommodate changes in cyber threat actors or capabilities that could threaten the alliance.

operations via trojans.[100] Information of increased malware activity before elections can serve as a warning to defenders that they should expect an increase in attacks before elections.

In lieu of the PMESII model, an alternative approach that could be used to order I&W indicators is to categorize them in three groups: strategic, technical, and operational. Strategic indicators can include, for example, new sanctions against North Korea or national elections. Technical indicators can comprise specific observable indicators, such as email addresses used when registering the domains and names of domains in C2 of attacks. Operational indicators can include, for example, financial resources flowing into hacker units.

Suggested actions: When forming the indicators for various cyber scenarios, analysts should incorporate military, social, and geopolitical indicators by grouping them into comprehensive categories, such as the ones offered by the PMESII model, or by ordering the indicators into strategic, technical, and operational. NATO is unlikely to see cyberattacks "exclusively as the basis of attacks against us as an Alliance"; instead, such attacks are going to be correlated with activities outside of cyberspace.[101] Therefore, NATO entities should consider supplementing their technical sources of I&W information with intelligence-based I&W assessing the geopolitical environment, providing advance notice of increasing geopolitical tensions and potentially follow-on serious cyberattacks and cyberconflict.

Besides being comprehensive, NATO's I&W framework should be flexible to accommodate changes in cyber threat actors or capabilities that could threaten the alliance. NATO's I&W framework should also be scalable, in order to have the capacity to accommodate and manage the rapid growth of internet-connected devices and new NATO-critical sites that increase the target surface for malicious cyber activities. To manage the growing number of assets and the respective increase in data flow, NATO entities should periodically reevaluate the indicators and prioritization of data collection resources, techniques, and methods.

Step 5: Establish Data Collection Methods and Sources; Set up a Collection Requirement and Prioritization Matrix

While the capabilities may exist in a developing stage, I&W analysts should establish viable and reliable data sources for each indicator, such as dark web data, malware intelligence reporting and social media data, and network traffic and system logs provided through various threat intelligence platforms.[102] Each indicator should have at least one periodically updated source. Moreover, due to the continuously evolving cyber threats to the alliance, the content and nature of I&W should be continuously updated and adjusted accordingly. Because of the variety of indicators, NATO entities may choose to collect data for each of the indicators through different sources, internal or external to NATO's entities.

One of the consequences of the explosion of information generation is the ability to analyze the data for law enforcement, national security, and intelligence purposes. For example, open source intelligence (OSINT) tools have been developed to mine not only social media but also countless other sources of publicly available information (e.g., news articles, shipping manifests, court records). In addition, those same OSINT tools can be very effective for I&W, to provide early warnings of an impending assault or use during ongoing operations as a way to provide indications that one's forces or actions have been discovered. For example, during the U.S. raid that captured Osama bin Laden in 2011, one resident posted a message to social media (Twitter) complaining about the noise of helicopters over his house.[103] And, in late 2018, a British amateur photographer tweeted a photograph of a strange airplane flying overhead.[104] Only later did he realize it was flying the U.S. President to Iraq for a secret meeting.

Some of the methods used to analyze these data sets include machine learning, statistical analytics (to include time series and linear regression), sentiment analysis, belief rule-based models, and evolutionary computing.[105] For example, social sentiment analysis can be applied to social media data to track and warn of discourse that could trigger a cyberattack. Sentiment analysis identifies opinions in text and can be used to differentiate between positive and negative cybersecurity-oriented tweets on Twitter. The analysis can then be used to create a social sentiment sensor to detect increases in overly negative discourse on cybersecurity-relevant themes. Sentiment analysis can be especially effective when combined with network analysis to identify social groups, geolocation tagging to identify the location of the group, and machine-learning techniques to automate the analytical process.[106] Monitoring cybersecurity discourse on Twitter could be an indicator that falls in the *social* category of the PMESII model.

Another example of a technique that can facilitate the prediction of cyberattacks is machine learning. A supervised machine learning system can be used to predict the initial stages of an attack and recognize patterns of previously unknown large-scale attacks before they have occurred. It does this, in part, by detecting attacks early and creating a model for future detection of similar attacks. Machine learning techniques have two main stages. First, a sample of data is fed into a machine learning module to train the machine to recognize attack sequences. Second, the machine applies this training to new data and detects similar attack patterns.[107] For example, in the case of the 2017 ransomware campaign known as WannaCry, a cybersecurity company used a machine learning module to collect initial data on infected computers, create a detection module, and then distribute that module to its not-yet-infected clients, who used the module to prevent WannaCry from infecting their networks.[108]

Suggested actions: To ensure access to comprehensive information, NATO networks should integrate data they collect with open-source intelligence and private-sector strategic and cyber threat intelligence indicators.[109] NATO entities should also continue to work toward improving their internal technical monitoring and may consider

To enhance cyber defenses across all member states, NATO entities should consider designing a Smart Defence initiatve for exchange of I&W data, I&W methodologies, and best practices.

increasing their reliance on private-sector products to enhance their I&W capabilities. For example, cybersecurity companies are developing, providing, and maintaining advanced network defense techniques where they use innovative methods to derive data and indicators, such as using machine learning techniques or monitoring and collecting data from the deep and dark web.[110] There are many commercial companies in the cybersecurity space providing a variety of I&W services. Offerings include secure infrastructure, including endpoint, application-level, cloud, and mobile device monitoring. Private sector products span the entire cyber kill chain: from threat intelligence services to detecting and preventing anomalous and malicious behavior and remediating and performing forensic investigation after an attack has occurred.[111] These private-sector companies and their capabilities should be used only to *supplement* existing NATO capabilities, rather than to actually *conduct* I&W operations on behalf of NATO or another government entity.

To enhance cyber defenses across all member states, NATO entities should consider designing a Smart Defence initiative for the exchange of I&W data, methodologies, and best practices. Such projects become critical efforts that will increase the overall ability of the alliance to defend itself by strengthening the weakest links. They currently cover the Smart Defence Multinational Cyber Defence Capability Development, the Malware Information Sharing Platform project, and the Multinational Cyber Defence Education and Training project.[112] NATO can establish and support an I&W methodologies and best practices project in which nations that have led in developing and implementing I&W capabilities in cyberspace can help other NATO members in developing, improving, and integrating such I&W capabilities in their national cyber defense strategies and centers. It would enable the maintenance and improvement of situational awareness of NATO networks, as well as networks of individual NATO members as they are linked to and affect NATO's infrastructure. A potential challenge when setting up this collaborative framework may originate from issues of trust when sharing sensitive cyber I&W data, timelines for executing such sharing initiatives, and actionability among the 29 NATO nations. NATO's other Smart Defense projects have demonstrated an ability to overcome these potential roadblocks. Therefore, drawing lessons from the implementation and development of NATO's other Smart Defense projects can provide useful guidelines for how to overcome similar concerns when setting up a cyber I&W Smart Defense project.

NATO's entities can spearhead the construction of uniform trusted information-sharing capabilities between alliance entities and NATO members, as well as partner nations. The continuous and streamlined sharing of standardized cyber I&W data across NATO entities and across member states will facilitate the accumulation of valuable data on malicious cyber incidents across NATO's networks, thus enhancing shared situational awareness and serving to better identify the most targeted areas of the alliance's networks.

Step 6: Establish Standard Operating Procedures and Exercise Chain of Communication and Command in Different Scenarios

At this stage, NATO's cyber I&W analysts should identify specific actions to be taken if a particular warning of a cyber threat scenario occurs. To ensure the information is relayed through the appropriate channels to the relevant decisionmaking structures as rapidly as possible, NATO should establish and practice international incident response procedures.

NATO has a mandate to provide coordinated assistance to its member states in the event of a cyber crisis and has initiated relevant activities aimed to enhance collective incident response. One example is the creation of a cyber defense framework through an MOU, which was developed in 2015 and is currently being updated. NATO also has Cyber Rapid Reaction teams available to assist member states in the event of cyberattacks.[113] Furthermore, NATO's Policy on Cyber Defense states that that the North Atlantic Council will adjudicate on any collective response and that NATO will maintain strategic ambiguity regarding its type of response in different scenarios—a prudent approach from the perspective of deterrence. To that effect, there are no publicly available international incident response plans that delineate the specific roles and responsibilities of NATO entities or member nations in case of international incident response to different types of cyberattacks.[114]

While the MOU provides a forum for strategic discussion and NATO has set up some formal guidelines on decisionmaking authorities, there is uncertainty regarding the ability of the alliance and its members to effectively implement these strategies in a large-scale cyber crisis in real time. Consequently, member states are not receiving consistent and specific guidelines on how to align their incident response policies with those of NATO and other member states to facilitate international collaboration in times of crisis. It is worth reiterating that although the alliance develops and exercises C2 and supporting capabilities for joint, combined operations, decisionmaking stays with each NATO member state. Therefore, NATO members often operate alone or through bilateral or multilateral cooperation with other nations outside of NATO's context.[115]

Suggested actions: Although NATO does not have authority to force its members into implementing specific cyber incident response requirements in cross-border cyber crises, the alliance could offer guidance to national leaders on how to reduce cyber risks in defense-related national sectors such as energy and transportation. NATO can, for example, enhance collaboration on identifying interdependencies between the services it offers to its members and the members' networks that support these services. NATO can also set up alliance-wide minimum cybersecurity standards that each nation would be advised to implement to prepare for international cyber incident response.[116] Frameworks and recommendations already developed by the U.S. Department of Homeland Security, U.S. National Institute for Standards and Technology, and the SANS Institute, among others, can provide a useful starting point for the development of such NATO standards.[117] NCIRC can be involved in monitoring the implementation of such guidelines and in providing feedback and disseminating best practices to members, which could be helpful for improving their incident response policies.[118]

In designing international incident response procedures, NATO entities should consider outlining clear thresholds for the magnitude of attacks and the respective responses each could trigger, differentiate between cyber-espionage and cyberattacks, and design different protocols of operation in each scenario. All of these considerations should be discussed among the NATO bodies and should be implemented in advance of any significant cyber threats to ensure NATO entities, member states, and partners are aware of their responsibilities and ready to act in case of an actual cyber threat.

Besides establishing these operational procedures, NATO entities and member states should consider practicing their application in different scenarios. Such processes should enable fast decisionmaking to allow for decision-makers to consider all viable options with as much time as possible.[119] Therefore, cyber I&W frameworks have to be integrated in the existing chain of command and communication structure and in NATO's crisis response processes, planning, and missions, with clear communication protocols and designated information recipients to ensure timely transfer of information. Such processes can be set up, integrated, and practiced during NATO-wide exercises, such as the NATO annual Crisis Management Exercise, which has been taking place since 1992 to test NATO's consultation and decisionmaking procedures at the strategic military and political level, within NATO and between NATO and partner nations.[120]

General Recommendations for Improving I&W Cyber Frameworks

To ensure the necessary prioritization, shared understanding and effective establishment of robust cyber I&W frameworks, the alliance should foster high levels of personnel readiness through training, education, and regularly held joint exercises. Such continuous cyber education, exercises, and training, with a focus on defensive posture, could be spearheaded by NATO's CCDCOE. NATO's Supreme Allied Commander delegated to CCDCOE the coordination of all cyber training and education for cyber defense operations within the alliance. CCDCOE, therefore, is well-positioned to spearhead and coordinate an effort to integrate reporting on and implementation and integration of I&W capabilities across the different educational institutions of the alliance.[121] Besides education, exercises for incorporating cyber I&W in planning and operations should be integrated into trainings at the tactical, operational, and strategic levels.

To improve cyber I&W concepts and facilitate their implementation and integration, NATO should consider standardizing the key cyber I&W terminology and publicizing a formal definition of cyber I&W across the alliance. A common legal foundation will ensure a level of uniformity of the discipline across NATO entities and member states and will improve the effectiveness of collaboration and data exchange through improved shared understanding.

NATO may further consider recommending the prioritization of various indicators against cyber threats by including them in NATO's Defense Planning Process in addition to defining targets for members' implementation of national cyber defense capabilities.[122]

Conclusion

NATO should consider further integrating cyber situational awareness in the traditional situational awareness processes of the alliance. NATO has a relatively mature and robust approach to situational awareness, which is not only about missions and threats but also covers network status. More in-depth awareness of how NATO's networks are operating and how they are secure, what the interdependencies are of the different components of NATO's networks, and how a compromise on some of them would affect the rest can be valuable, especially given the tightly linked and integrated elements of the cyber domain.

Conclusion

This perspective has provided three viewpoints on characterizing NATO's past, present, and emerging position in cyberspace. In preparation for maintaining and preserving these strong alliances and capabilities, NATO has already made many foundational steps toward preparing itself for operating effectively in cyberspace. From the Wales Summit in 2014, where a cyber action plan was first adopted, to the Warsaw Summit in 2016, where nations agreed to strengthen their cyber defenses and recognize cyber as a domain of operation, to the Brussels Summit in 2018, where the CyOC was created, each of these actions has helped foster a capable and successful workforce, leadership, and command structure for cyberspace operations.

In addition, a concern of particular importance is developing an effective cyber I&W capability that can provide advance warning of malicious cyberactivity and detect civilian or military observation of NATO operations. Effective I&W provides more than warning; it also supports a timely and clear gauge of indications and intensions that are important in managing friction during a suspected cyber event while also providing confidence for deescalation. While cyber may represent a new domain of operations for NATO, it is similarly new for all countries and alliances across the globe. And even though the way ahead may be cloudy and difficult, NATO has made important advances that ensure its persistence as a strong defensive military alliance in the face of dynamic attack surfaces, emerging technologies, and escalating malicious cyberactivity.

But time will not stop. These and other efforts focus on enabling embryonic capabilities to face the alliance's short-term needs. Cyber as a domain of military operation is very rapidly evolving, based heavily on technology, with low barriers to entry (for attackers), and has limited warfare doctrine and experience. Therefore, NATO needs to quickly catch up by urgently programming warfare development efforts (e.g., areas such as research and development, concept development, feasibility studies, experimentation and demonstration) to effectively anticipate adversaries' intentions, disrupt their activities, and provide on-time capabilities to the warfighter.

Notes

[1] Bruce Konviser, “Czechs to Train, Lead Arms Unit for NATO,” *Chicago Tribune*, December 22, 2003.

[2] NATO began to focus on the potential challenges posed by weapons of mass destruction in the early 1990s, as NATO’s 1991 Strategic Concept identified proliferation of nuclear, biological, and chemical weapons as a problem requiring alliance attention (Ashton B. Carter and David B. Omand, “Countering the Proliferation Risks: Adapting the Alliance to the New Security Environment,” *NATO Review*, No. 5, Vol. 44, September 1996, pp. 10–15).

[3] Carter and Omand, 1996. The DGP has since been reorganized as the Committee on Proliferation, which meets in two formats, Defense and Politico-Military.

[4] “Washington Summit Communique,” North Atlantic Council, Washington, D.C., April 24, 1999. The initiative included, among other things, establishment of a WMD Centre within the International Staff and plans to enhance existing allied ability to operate under the threat of WMD and to help coordinate civil protection against WMD risks.

[5] The U.S. goal, in the words of one senior U.S. official, was to “deconstruct . . . the old NATO to build a new one to meet the threat of terrorism and weapons of mass destruction.” (U.S. Ambassador to NATO Nicholas Burns, quoted in Robert G. Kaiser and Keith B. Richburg, “NATO Looking Ahead to a Mission Makeover,” *Washington Post*, November 5, 2002.)

[6] George Robertson, “Tackling Terror: NATO’s New Mission,” speech at the American Enterprise Institute, Washington, D.C., June 20, 2002, June 25, 2002. Initiatives included a Prototype Deployable Nuclear, Biological, Chemical (NBC) Analytical Laboratory; a Prototype NBC Event Response team; a virtual Center of Excellence for NBC Weapons Defense, a NATO Biological and Chemical Defense Stockpile, and a Disease Surveillance system (NATO, “Prague Summit Declaration, Issued by the Heads of State and Government Participating in the Meeting of the North Atlantic Council in Prague, Czech Republic,” November 21, 2002).

[7] Eric Terzuolo, *NATO and Weapons of Mass Destruction: Regional Alliance, Global Threats*, Abingdon-on-Thames: Routledge, 2006, p. 122.

[8] “NATO Multinational Chemical, Biological, Radiological and Nuclear Defence Battalion,” SHAPE, updated 2018.

[9] Terzuolo, 2006, p. 122.

[10] “NATO Multinational Chemical, Biological, Radiological and Nuclear Defence Battalion,” 2018; George Robertson, “Launch of NATO CBRN Defense Battalion,” remarks, December 1, 2003.

[11] Paul Gallis, *The NATO Summit at Prague, 2002*, Congressional Research Service (CRS), March 1, 2005.

[12] “Combined Joint Chemical, Biological, Radiological and Nuclear Defence Task Force” *NATO Topics*, updated August 6, 2015.

[13] Natasha Lander and Burgess Laird, *Allied Defense Against the Unthinkable: Crafting NATO’s Role in Countering Chemical and Biological Threats*, Santa Monica, Calif.: RAND Corporation, 2018, unavailable to the general public.

[14] Ann Scott Tyson, “In New NATO, a Division of Military Labor,” *Christian Science Monitor*, November 27, 2002.

[15] Terzuolo, 2006, p. 121.

[16] “Defence Against Terrorism Programme of Work” NATO, updated July 3, 2018.

[17] Lander and Laird, 2018.

[18] Terzuolo, 2006, p. 121.

[19] The Joint Chiefs of Staff Joint Publication *Operations in Chemical, Biological, Radiological, and Nuclear Environments*, for example, notes of alliance and coalition operations that “when conducting combat operations, the JFC [Joint Forces Command] should consider the capabilities and limitations of all available forces to maximize their contributions and minimize their vulnerabilities. Peacetime activities with multinational partners, particularly multinational and interagency training and planning exercises, provide means of preparing for multinational combat operations in CBRN environments” (U.S. Joint Chiefs of Staff, *Operations in Chemical, Biological, Radiological, and Nuclear Environments*, Joint Publication 3-11, Washington, D.C., October 29, 2018, II-18).

[20] Konviser, 2003.

[21] Konviser, 2003 .

[22] “Combined Joint Chemical, Biological, Radiological and Nuclear Defence Task Force,” 2015.

[23] Terzuolo, 2006, p. 123.

[24] Lander and Laird, 2018.

[25] NATO, "Science for Peace and Security," webpage, updated October 12, 2018d. Key areas of focus included protection against CBRN agents, as well as diagnosing their effects, detection, decontamination, destruction, disposal and containment; risk management and recovery strategies and technologies; and medical countermeasures for CBRN agents.

[26] NATO School Oberammergau, *Course Catalogue*, 2019.

[27] Lander and Laird, 2018 .

[28] NATO, *The Prague Summit and NATO's Transformation: A Reader's Guide*, 2003; the strategy was updated in 2016 (North Atlantic Military Committee, "Military Committee Concept for Counter-Terrorism," approved January 6, 2016).

[29] NATO, "NATO Publishes New Policy to Combat Weapons of Mass Destruction Proliferation," press release, August 31, 2009.

[30] Lander and Laird, 2018.

[31] NATO HQ Consultation, Command and Control Staff, *Warning and Reporting and Hazard Prediction of Chemical, Biological, Radiological and Nuclear Incidents (Operators Manual*), ATP-45 Edition E, NATO, January 2014.

[32] Pavel Otrisal, "Selected Software Tools Used for CBRN Situation Assessment Within CZECH Armed Forces Chemical Corps," *Journal of Defense Management*, Vol. 2, No. 3, 2012.

[33] *Newsletter*, Joint CBRN Defence COE, 2012. According to the newsletter, the COE has dedicated efforts to NATO's Lessons Identified/ Lessons Learned (LI/LL) process and the Concept Development and Experimentation (CD&E) process, two processes that inform the NDPP; the newsletter cites CD&E as one of the COE's most critical lines of effort.

[34] NATO, "Chemical, Biological, Radiological, and Nuclear (CBRN) Defense," Allied Joint Publication 3.8A (Archived), United Kingdom Ministry of Defense, March 2012.

[35] NATO, "Weapons of Mass Destruction," December 8, 2017b.

[36] Pavel David, "CBRN Warning and Reporting Specialist Course," JCBRN Defense COE, October 2013.

[37] Lander and Laird, 2018, p. 9.

[38] NATO "Cyber Defense," webpage, updated July 16, 2018c.

[39] NATO, 2018c.

[40] NATO, 2018c.

[41] NATO, 2018c.

[42] Note that this view implicitly includes the notion of maintaining scope and context of NATO member countries' security posture, as discussed further below.

[43] NATO Standardization Agency, *AAP-06 NATO Glossary of Terms and Definitions*, 2018 edition, 2018.

[44] See, for example, Carson Zimmerman, *Ten Strategies of a World-Class Cybersecurity Operations Center*, MITRE Corporation, Bedford, Mass., 2014, pp. 315–316.

[45] Most are publicly available at NATO's E-Library webpage, last updated November 10, 2017a.

[46] James N. Mattis, "News Conference by Secretary Mattis at NATO Headquarters, Brussels, Belgium," October 4, 2018.

[47] "NATO Defence Planning Process," NATO, updated June 28, 2018.

[48] NATO, "Trident Juncture 18," fact sheet, October 31, 2018f.

[49] NATO, "Joint Press Conference with NATO Secretary General Jens Stoltenberg and the Minister of Defence of Norway, Frank Bakke-Jensen, at the Trident Juncture 2018 Distinguished Visitors' Day," press release, October 29, 2018.

[50] NATO Communications and Information Agency, "NCI Agency Responds to Fictional Threats in Successful Cyber Exercise," press release, December 11, 2018.

[51] Don Lewis, "What Is NATO Really Doing in Cyberspace?" *War on the Rocks*, February 4, 2019.

[52] NATO Allied Command Transformation Public Affairs Officer, "SACT and the Estonian Minister of Defence Sign an Agreement to Establish the NATO Cyber Range Capability," press release, September 8, 2014.

[53] NATO, "NATO Breaks Ground on Portugal IT Academy," press release, May 23, 2017.

[54] (ISC)2, *Cybersecurity Professionals Focus on Developing New Skills as Workforce Gap Widens: (ISC)2 Cybersecurity Workforce Study 2018*, October 17, 2018.

[55] See this overview of the DoD Cyber Workforce Framework: Chief Information Officer, U.S. Department of Defense, "About the DoD Cyber Workforce," fact sheet, undated.

[56] For information on the Defense Digital Service, a component of the U.S. Digital Service, see Defense Digital Service, "Transforming Technology Within the Department of Defense," fact sheet, undated.

[57] Office of the Under Secretary of Defense for Personnel and Readiness, "SECDEF Executive Fellows," webpage, undated.

[58] Author correspondence with a cybersecurity expert, December 17, 2018; Blake Moore, Cody Barrow, Andrea Little Limbago, Lonnie Garris, Jeremy Erb, Terry Roberts, and Kevin Zerrusen, *A Framework for Cyber Indications and Warning*, Intelligence and National Security Alliance Cyber Council, October 2018, p. 1.

[59] Email communication with a NATO representative, December 4, 2018; correspondence with a cybersecurity expert, December 17, 2018; Moore et al., 2018, p. 3.

[60] U.S. Joint Chiefs of Staff, Joint Intelligence, Joint Publication 2-0, Washington, D.C., October 22, 2013.

[61] U.S. Joint Chiefs of Staff, *Cyberspace Operations*, Joint Publication 3-12, Washington, D.C., June 8, 2018.

[62] Email communication with a NATO representative, December 4, 2018.

[63] NATO Standardization Agency, 2018.

[64] NATO Standardization Agency, 2018 .

[65] Intelligence and National Security Alliance, "Building a Stronger Intelligence Community," webpage, undated.

[66] Moore et al., p. 3.

[67] Bilyana V. Lilly, Lillian Ablon, Quentin E. Hodgson, and Adam S. Moore, "Applying Indications & Warning Frameworks to Cyber Incidents," 11th International Conference on Cyber Conflict, Tallinn, Estonia: NATO CCD COE Publications, forthcoming.

[68] NATO, 2018c.

[69] NATO, 2018c.

[70] NATO, "Brussels Summit Declaration," declaration following meeting of the North Atlantic Council, Brussels, July 11–12, 2018, July 11, 2018b.

[71] NATO, 2018b.

[72] NATO, 2018b; NATO Communications and Information Agency, "Cyber Security," webpage, undated; based on information provided by a NATO representative in communication with Bilyana Lilly, December 6, 2018.

[73] NCI Agency, "NIAS '17 – Mr Ian West," YouTube, November 30, 2017, timestamp 4:30.

[74] NATO, 2018f; CERT LV, "Brad Bigelow, Kiberšahs 2018," YouTube, October 18, 2018, timestamp 14:20 to 15:13.

[75] Email communication with a NATO representative, December 4, 2018.

[76] Brad Bigelow, "Mission Assurance: Shifting the Focus of Cyber Defense," in H. Rõigas, R. Jakschis, L. Lindström, and T. Minárik, eds., *Defending the Core: Proceedings of the 9th International Conference on Cyber Conflict*, Tallinn: NATO CCD COE Publications, 2017.

[77] Email communication with NATO representative, December 4, 2018.

[78] Email communication with NATO representative, December 4, 2018.

[79] NCISS will be relocated to Oeiras, Portugal, where a NATO training facility is currently being built. The facility is expected to be fully operational by the end of 2019, and its curriculum will be redesigned to focus more on the provision of cyber defense education and training. NATO Communications and Information Agency, "NATO Breaks Ground on Portugal IT Academy," press release, May 23, 2017; NATO, 2018d.

[80] NATO, 2018d.

[81] Per "Smart Defence," webpage, *NATO Review*, undated, "Smart defence is a concept that encourages Allies to cooperate in developing, acquiring and maintaining military capabilities to meet current security problems in accordance with the new NATO strategic concept."

[82] NATO, 2018d.

[83] Jan Goldman, ed., A*nticipating Surprise: Analysis for Strategic Warning*, Washington, D.C.: Joint Military Intelligence College, 2002.

[84] Cynthia Grabo, *Warning Intelligence*, McLean, Va.: Association of Former Intelligence Officers, 1987; Jonathan Lockwood, "The Application of LAMP," webpage, 2010; Jonathan Lockwood, "The Lockwood Analytic Method for Prediction (LAMP): An Innovative Methodological Approach to the Problem of Predictive Analysis," slide presentation, ANSER Analytic Services, January 2002.

[85] Moore et al., 2018.

[86] We recognize that there may not always be enough time in the cyber domain to deliberate very long on each of these steps, since actions need to be taken more quickly to defend the domain when attacked.

[87] For an example of a similar cyber I&W framework and its application to a real-word cyberincident, see Lilly et al., forthcoming.

[88] CERT LV, 2018, timestamp 11:00–11:45.

[89] Numbers of suspicious activities vary widely, based on definitions and scope, including the types of activities included in the estimation and the networks against which these activities are leveraged. Therefore, this figure should be considered as an aggregate number that represents only one variation of the estimate on the malicious activities performed against NATO's networks and other assets. "Brad Bigelow, Kiberšahs 2018," 2018, timestamp 11:00–11:45; NCI Agency, 2017, timestamp 10:20–10:30.

[90] "Brad Bigelow, Kiberšahs 2018," 2018, timestamp 11:00–11:45.

[91] NATO, 2018d; the alliance should prioritize targets, including facilities, devices, systems, networks, and services, that are most critical for fulfilling NATO's mission of collective defense and, if compromised, can trigger an Article 5 response.

[92] Franklin D. Kramer, Robert J. Butler, and Catherine Lotrionte, *Cyber and Deterrence: The Military-Civil Nexus in High-End Conflict*, Atlantic Council, Brent Scowcroft Center on International Security, January 2017, p. 5; Tim Prior, *NATO: Pushing Boundaries for Resilience*, Center for Security Studies, Zürich: ETH Zürich, July 13, 2018.

[93] "Allies and Partners Address Critical Infrastructure and a Key Enabler to Enhance Resilience," press release, North Atlantic Treaty Organization, December 10, 2018.

[94] "Allies and Partners Address Critical Infrastructure and a Key Enabler to Enhance Resilience," 2018.

[95] Moore et al., 2018, p. 12; MITRE's ATT&CK and PRE-ATT&CK frameworks are the most comprehensive open-source frameworks of tactics and techniques used by attackers along the cyber kill chain (MITRE Corporation, "PRE-ATT&CK Techniques," database, undated). They are useful for those cyber defenders who are involved at the tactical and hands-on level to identify techniques used by attackers and prevent or mitigate attacks.

[96] NATO, 2018d.

[97] NATO, 2018d.

[98] For example, see Cylance, *Operation Cleaver*, undated, pp. 74–76, for a list of hundreds of indicators of compromise from known advanced persistent threat.

[99] Leekyung Ko, "North Korea as a Geopolitical and Cyber Actor: A Timeline of Events," New America, Washington, D.C., June 6, 2018.

[100] Kenneth Geers and Nadiya Kostyuk, "Hackers Are Using Malware to Find Vulnerabilities in U.S. Swing States. Expect Cyberattacks," *Washington Post*, November 5, 2018.

[101] "Brad Bigelow, Kiberšahs 2018," 2018, timestamp 11:40–12:00.

[102] One such platform is FireEye's iSIGHT (FireEye, "FireEye iSIGHT Threat Intelligence: Forward-Looking Threat Intelligence with Highly Contextual Analysis," fact sheet, 2018).

[103] Jethro Mullen and Sophia Saifi, "Whatever Happened to Guy Who Tweeted About Raid That Killed Osama bin Laden?" CNN, January 20, 2016.

[104] Mark Moore, "Photographer Spotted Air Force One En Route to Trump's Surprise Iraq Visit," *New York Post*, December 27, 2018.

[105] Drew Robb, "Eight Top Threat Intelligence Platforms," eSecurity Planet newsletter, July 18, 2017; Martin Husak, Jana Komarkova, Elias Bou-Harb, and Pavel Celeda, "Survey of Attack Projection, Prediction, and Forecasting in Cyber Security," *IEEE Communications Surveys and Tutorials*, Vol. 21, No. 1, September 2018, p. 15.

[106] Aldo Hernandez-Suarez, Gabriel Sanchez-Perez, Karina Toscano-Medina, Victor Martinez-Hernandez, Hector Perez-Meana, Jesus Olivares-Mercado, and Victor Sanchez, "Social Sentiment Sensor in Twitter for Predicting Cyber-Attacks Using L1 Regularization," *Sensors* (Basel), Vol. 18, No. 5, May 2018, p. 1380.

[107] Husak et al., 2018, p. 12.

[108] Correspondence with a cybersecurity expert from the private sector, December 21, 2018.

[109] As a SANS Survey conducted in March and April 2018 and based on responses from 277 IT professionals from Europe, the United States, and Asia reveals, 26 percent of cyberattacks were discovered through endpoint detection and response platforms (Lee Neely, *Endpoint Detection and Response: A SANS Survey*, SANS Institute, SANS Analyst Program, June 2018; Nate Lord, "What is Endpoint Detection and Response? A Definition of Endpoint Detection and Response," Data*Insider*, Digital Guardian, January 3, 2019).

[110] Melissa E. Hathaway, "Preface," *Proceedings of Advanced Research Workshop*, Geneva, Switzerland, September 11–13, 2013.

[111] Robb, 2017; "CylancePROTECT: Continuous Threat Protection Powered by Artificial Intelligence," fact sheet, Cylance, Irvine, Calif., 2018.

[112] NATO, 2018d.

[113] NATO, 2018d.

[114] Matthew W. Holt, "Aligning National Cyber Security Strategies to International Guidance: A First Step Toward Improving Incident Response Capabilities Across NATO," in Melissa E. Hathaway, ed., *Best Practices in Computer Network Defense: Incident Detection and Response*, Amsterdam: IOS Press, 2014, p. 72.

[115] Holt, 2014, pp. 72–73.

[116] Holt, 2014, p. 74.

[117] U.S. Department of Homeland Security, "National Cyber Incident Response Plan," December 2016; Paul Cichonski, Tom Millar, Tim Grance, and Karen Scarfone, *Computer Security Incident Handling Guide: Recommendations of the National Institute of Standards and Technology*, U.S. Department of Commerce, National Institute of Standards and Technology, Special Publication 800-61, Revision 2, August 201; Patrick Kral, *Incident Handler's Handbook*, SANS Institute, 2019.

[118] Holt, 2014, p. 75.

[119] "Brad Bigelow, Kiberšahs 2018," 2018, timestamp 12:21–12:33.

[120] "Crisis Management Exercise 2017," press release, NATO, September 28, 2017.

[121] Kimberly Underwood, "NATO Strengthens Its Cyber Stance," blog post, *Cyber Edge*, April 1, 2018.

[122] NATO, 2016b.

References

Bigelow, Brad, "Mission Assurance: Shifting the Focus of Cyber Defense," in H. Rõigas, R. Jakschis, L. Lindström, and T. Minárik, eds., *Defending the Core: Proceedings of the 9th International Conference on Cyber Conflict*, Tallinn: NATO CCD COE Publications, 2017. As of May 13, 2019:
https://ccdcoe.org/uploads/2018/10/Art-03-Mission-Assurance-Shifting-the-Focus-of-Cyber-Defence.pdf

Carter, Ashton B., and David B. Omand, "Countering the Proliferation Risks: Adapting the Alliance to the New Security Environment," *NATO Review*, Vol. 44, No. 5, September 1996, pp. 10–15.

CERT LV, "Brad Bigelow, Kiberšahs 2018," YouTube video, October 18, 2018. As of April 8, 2019:
https://www.youtube.com/watch?v=ULrwyi08rJk

Chief Information Officer, U.S. Department of Defense, "About the DoD Cyber Workforce," webpage, undated. As of May 7, 2019:
https://dodcio.defense.gov/Cyber-Workforce.aspx

Cichonski, Paul, Tom Millar, Tim Grance, and Karen Scarfone, *Computer Security Incident Handling Guide: Recommendations of the National Institute of Standards and Technology*, U.S. Department of Commerce, National Institute of Standards and Technology, Special Publication 800-61, Revision 2, August 2012. As of April 10, 2019:
https://nvlpubs.nist.gov/nistpubs/specialpublications/nist.sp.800-61r2.pdf

"Combined Joint Chemical, Biological, Radiological and Nuclear Defence Task Force," *NATO Topics*, updated August 6, 2015. As of May 7, 2019:
https://www.nato.int/cps/en/natohq/topics_49156.htm

"Crisis Management Exercise 2017," press release, North Atlantic Treaty Organization, September 28, 2017. As of April 10, 2019:
https://www.nato.int/cps/en/natohq/news_147373.htm

Cylance, *Operation Cleaver*, undated. As of April 8, 2019: https://www.cylance.com/content/dam/cylance/pdfs/reports/Cylance_Operation_Cleaver_Report.pdf

"CylancePROTECT: Continuous Threat Protection Powered by Artificial Intelligence," fact sheet, Cylance, Irvine, Calif., 2018. As of April 10, 2019: https://www.cylance.com/content/dam/cylance/pdfs/data_sheets/CylancePROTECT.pdf

David, Pavel, "CBRN Warning and Reporting Specialist Course," Joint Chemical Biological Radiological Nuclear Defense Center of Excellence, October 2013. As of May 7, 2019: https://www.jcbrncoe.cz/index.php/events-67/main-events-2013/226-cbrn-warning-and-reporting-specialist-course

"Defence Against Terrorism Programme of Work," North Atlantic Treaty Organization, updated July 3, 2018. As of May 7, 2019: https://www.nato.int/cps/us/natohq/topics_50313.htm

Defense Digital Service, "Transforming Technology Within the Department of Defense," webpage, undated. As of May 7, 2019: https://dds.mil

FireEye, "FireEye iSIGHT Threat Intelligence: Forward-Looking Threat Intelligence with Highly Contextual Analysis," fact sheet, 2018. As of April 10, 2019: https://www.fireeye.com/content/dam/fireeye-www/products/pdfs/pf/intel/ds-isight-threat-intelligence.pdf

Gallis, Paul, *The NATO Summit at Prague*, 2002, Congressional Research Service, March 1, 2005. As of May 7, 2019: https://fas.org/sgp/crs/row/RS21354.pdf

Geers, Kenneth, and Nadiya Kostyuk, "Hackers Are Using Malware to Find Vulnerabilities in U.S. Swing States. Expect Cyberattacks," *Washington Post*, November 5, 2018.

Goldman, Jan, ed., *Anticipating Surprise: Analysis for Strategic Warning*, Washington, D.C.: Joint Military Intelligence College, 2002.

Grabo, Cynthia, *Warning Intelligence*, McLean, Va.: Association of Former Intelligence Officers, 1987.

Hathaway, Melissa E., "Preface," *Proceedings of Advanced Research Workshop*, Geneva, Switzerland, September 11–13, 2013. As of April 10, 2019: https://www.nato.int/nato_static_fl2014/assets/pdf/pdf_2014_04/20140513_140428-computer-network-defense-preface.pdf

Hernandez-Suarez, Aldo, Gabriel Sanchez-Perez, Karina Toscano-Medina, Victor Martinez-Hernandez, Hector Perez-Meana, Jesus Olivares-Mercado, and Victor Sanchez, "Social Sentiment Sensor in Twitter for Predicting Cyber-Attacks Using L1 Regularization," *Sensors* (Basel), Vol. 18, No. 5, May 2018, p. 1380. As of April 10, 2019: https://www.ncbi.nlm.nih.gov/pmc/articles/PMC5982517/

Holt, Matthew W., "Aligning National Cyber Security Strategies to International Guidance: A First Step Toward Improving Incident Response Capabilities Across NATO," in Melissa E. Hathaway, ed., *Best Practices in Computer Network Defense: Incident Detection and Response*, Amsterdam: IOS Press, 2014, p. 72.

Husak, Martin, Jana Komarkova, Elias Bou-Harb, and Pavel Celeda, "Survey of Attack Projection, Prediction, and Forecasting in Cyber Security," *IEEE Communications Surveys and Tutorials*, Vol. 21, No. 1, September 2018. As of May 7, 2019: https://ieeexplore.ieee.org/document/8470942

Intelligence and National Security Alliance, "Building a Stronger Intelligence Community," webpage, undated. As of April 8, 2019: https://www.insaonline.org/

(ISC)2, *Cybersecurity Professionals Focus on Developing New Skills as Workforce Gap Widens: (ISC)2 Cybersecurity Workforce Study 2018*, October 17, 2018. As of December 27, 2018: https://www.isc2.org/-/media/7CC1598DE430469195F81017658B15D0.ashx

Kaiser, Robert G., and Keith B. Richburg, "NATO Looking Ahead to a Mission Makeover," *Washington Post*, November 5, 2002. As of May 7, 2019: https://www.washingtonpost.com/archive/politics/2002/11/05/nato-looking-ahead-to-a-mission-makeover/84f6164d-22c2-4bc8-9f5d-2a7fa92793db/?utm_term=.081d091ce230

Ko, Leekyung, "North Korea as a Geopolitical and Cyber Actor: A Timeline of Events," webpage, New America, Washington, D.C., June 6, 2018. As of April 9, 2019: https://www.newamerica.org/cybersecurity-initiative/c2b/c2b-log/north-korea-geopolitical-cyber-incidents-timeline/

Konviser, Bruce, "Czechs to Train, Lead Arms Unit for NATO," *Chicago Tribune*, December 22, 2003. As of May 7, 2019: https://www.chicagotribune.com/news/ct-xpm-2003-12-22-0312220075-story.html

Kral, Patrick, *Incident Handler's Handbook*, SANS Institute, 2019. As of April 10, 2019: https://www.sans.org/reading-room/whitepapers/incident/incident-handlers-handbook-33901

Kramer, Franklin D., Robert J. Butler, and Catherine Lotrionte, *Cyber and Deterrence: The Military-Civil Nexus in High-End Conflict*, Atlantic Council, Brent Scowcroft Center on International Security, January 2017. As of April 8, 2019:
http://www.atlanticcouncil.org/images/publications/Cyber_and_Deterrence_web_0103.pdf

Lander, Natasha, and Burgess Laird, *Allied Defense Against the Unthinkable: Crafting NATO's Role in Countering Chemical and Biological Threats*, Santa Monica, Calif.: RAND Corporation, unavailable to the general public.

Lewis, Don, "What Is NATO Really Doing in Cyberspace?" *War on the Rocks*, February 4, 2019. As of February 5, 2019:
https://warontherocks.com/2019/02/what-is-nato-really-doing-in-cyberspace/

Lilly, Bilyana V., Lillian Ablon, Quentin E. Hodgson, and Adam S. Moore, "Applying Indications & Warning Frameworks to Cyber Incidents," 11th International Conference on Cyber Conflict, Tallinn, Estonia: NATO CCD COE Publications, forthcoming.

Lockwood, Jonathan, "The Lockwood Analytic Method for Prediction (LAMP): An Innovative Methodological Approach to the Problem of Predictive Analysis," slide presentation, ANSER Analytic Services, January 2002. As of April 8, 2019:
http://lamp-method.org/lampppt.ppt

———, "The Application of LAMP," webpage, 2010. As of April 8, 2019:
http://lamp-method.org/2.html

Lord, Nate, "What is Endpoint Detection and Response? A Definition of Endpoint Detection and Response," *DataInsider*, Digital Guardian, January 3, 2019. As of April 10, 2019:
https://digitalguardian.com/blog/what-endpoint-detection-and-response-definition-endpoint-detection-response

Mattis, James N., "News Conference by Secretary Mattis at NATO Headquarters, Brussels, Belgium," October 4, 2018. As of December 3, 2018:
https://dod.defense.gov/News/Transcripts/Transcript-View/Article/1654419/news-conference-by-secretary-mattis-at-nato-headquarters-brussels-belgium/

MITRE Corporation, "PRE-ATT&CK Techniques," database, undated. As of April 8, 2019:
https://attack.mitre.org/techniques/pre/

Moore, Blake, Cody Barrow, Andrea Little Limbago, Lonnie Garris, Jeremy Erb, Terry Roberts, and Kevin Zerrusen, *A Framework for Cyber Indications and Warning*, Intelligence and National Security Alliance Cyber Council, October 2018. As of April 8, 2019:
https://www.insaonline.org/wp-content/uploads/2018/10/INSA-Framework-For-Cyber-Indications-and-Warning.pdf

Moore, Mark, "Photographer Spotted Air Force One En Route to Trump's Surprise Iraq Visit," *New York Post*, December 27, 2018.

Mullen, Jethro, and Sophia Saifi, "Whatever Happened to Guy Who Tweeted About Raid That Killed Osama bin Laden?" CNN, January 20, 2016. As of January 9, 2019:
https://www.cnn.com/2016/01/20/asia/osama-bin-laden-raid-tweeter-sohaib-athar-rewind/index.html

NATO—*See* North Atlantic Treaty Organization.

NATO Communications and Information Agency, "Cyber Security," webpage, undated. As of April 8, 2019:
https://www.ncia.nato.int/Our-Work/Pages/Cyber-Security.aspx

———, "NATO Breaks Ground on Portugal IT Academy," press release, May 23, 2017. As of April 8, 2019:
https://www.ncia.nato.int/NewsRoom/Pages/170523-NCI-Academy_groundbreaking_ceremony.aspx

———, "NCI Agency Responds to Fictional Threats in Successful Cyber Exercise," press release, December 11, 2018. As of February 5, 2019:
https://www.ncia.nato.int/NewsRoom/Pages/20181211-CyberCoalition.aspx

"NATO Multinational Chemical, Biological, Radiological and Nuclear Defence Battalion," Supreme Headquarters Allied Powers Europe, updated 2018. As of May 7, 2019:
https://shape.nato.int/about/aco-capabilities2/nato-multinational-chemical--biological--radiological-and-nuclear-defence-battalion

NATO Standardization Agency, *AAP-06 NATO Glossary of Terms and Definitions*, 2018 edition, 2018.

North Atlantic Treaty Organization, "NATO Publishes New Policy to Combat Weapons of Mass Destruction Proliferation," press release, August 31, 2009. As of May 7, 2019:
https://www.nato.int/cps/en/natohq/news_57234.htm?selectedLocale=en

NATO School Oberammergau, *Course Catalogue*, 2019. As of May 7, 2019:
http://www.natoschool.nato.int/Academics/Portfolio/Course-Catalogue?keyword=CBRN&code=&startdate=&enddate=&exactdatematch=False&durationfrom=1&durationto=3084&residentcourse=True&onlinecourse=True&adlmodules=False&department=

NCI Agency—*See* NATO Communications and Information Agency.

Neely, Lee, *Endpoint Detection and Response: A SANS Survey*, SANS Institute, SANS Analyst Program, June 2018. As of April 10, 2019:
https://www.guidancesoftware.com/docs/default-source/document-library/publication/survey_endpoint-2018_opentext.pdf

Newsletter, Joint CBRN Defence COE, 2012.

NATO Communications and Information Agency, "NIAS '17—Mr Ian West," YouTube, November 30, 2017. As of April 8, 2019:
https://www.youtube.com/watch?v=BT7t0YID-So

NATO HQ Consultation, Command and Control Staff, *Warning and Reporting and Hazard Prediction of Chemical, Biological, Radiological and Nuclear Incidents (Operators Manual)*, ATP-45 Edition E, NATO, January 2014. As of May 7, 2019:
https://nhqc3s.hq.nato.int/Apps/Architecture/NISP2/std43.aspx?vndb=standards&vsbn=n&refid=nso-stanag2103ed11&sbbs=y

North Atlantic Military Committee, "Military Committee Concept for Counter-Terrorism," NATO, approved January 6, 2016. As of May 7, 2019:
https://www.nato.int/nato_static_fl2014/assets/pdf/topics_pdf/20160905_160905-mc-concept-ct.pdf

North Atlantic Treaty Organization, "Prague Summit Declaration, Issued by the Heads of State and Government Participating in the Meeting of the North Atlantic Council in Prague, Czech Republic," press release, November 21, 2002. As of May 7, 2019:
https://www.nato.int/cps/en/natohq/official_texts_19552.htm

———, *The Prague Summit and NATO's Transformation: A Reader's Guide*, 2003. As of May 7, 2019:
https://www.nato.int/docu/rdr-gde-prg/rdr-gde-prg-eng.pdf

———, "Chemical, Biological, Radiological, and Nuclear (CBRN) Defense," Allied Joint Publication 3.8A (Archived), United Kingdom Ministry of Defense, March 2012. As of May 7, 2019:
https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/628208/20130215-ajp3_8_A_cbrn.pdf

———, "E-Library," webpage, last updated November 10, 2017a. As of May 7, 2019:
https://www.nato.int/cps/en/natohq/publications.htm

———, "Weapons of Mass Destruction," webpage, December 8, 2017b. As of May 7, 2019:
https://www.nato.int/cps/en/natohq/topics_50325.htm

———, "NATO Defence Planning Process," webpage, updated June 28, 2018a. As of December 3, 2018:
https://www.nato.int/cps/en/natohq/topics_49202.htm

———, "Brussels Summit Declaration," meeting of the North Atlantic Council, Brussels, July 11–12, 2018, July 11, 2018b.

———, "Cyber Defense," webpage, updated July 16, 2018c. As of January 27, 2019:
https://www.nato.int/cps/en/natohq/topics_78170.htm

———, "Science for Peace and Security," webpage, updated October 12, 2018d. As of May 7, 2019:
https://www.nato.int/cps/en/natolive/78209.htm

———, "Joint Press Conference with NATO Secretary General Jens Stoltenberg and the Minister of Defence of Norway, Frank Bakke-Jensen, at the Trident Juncture 2018 Distinguished Visitors' Day," press release, October 29, 2018e. As of December 3, 2018:
https://www.nato.int/cps/en/natohq/opinions_159853.htm

———, "Trident Juncture 18," fact sheet, October 31, 2018f. As of December 3, 2018: https://www.nato.int/cps/en/natohq/news_158620.htm

———, "Allies and Partners Address Critical Infrastructure and a Key Enabler to Enhance Resilience," press release, December 10, 2018g. As of April 8, 2019:
https://www.nato.int/cps/en/natohq/news_161675.htm

North Atlantic Treaty Organization Allied Command Transformation Public Affairs Officer, "SACT and the Estonian Minister of Defence Sign an Agreement to Establish the NATO Cyber Range Capability," press release, September 8, 2014. As of December 3, 2018:
https://www.act.nato.int/sact-and-the-estonian-minister-of-defence-sign-an-agreement-to-establish-the-nato-cyber-range-capability

Office of the Under Secretary of Defense for Personnel and Readiness, "SECDEF Executive Fellows," webpage, undated. As of May 7, 2019:
https://prhome.defense.gov/Readiness/EducationTraining/SDEF.aspx

Otrisal, Pavel, "Selected Software Tools Used for CBRN Situation Assessment Within CZECH Armed Forces Chemical Corps," *Journal of Defense Management*, Vol. 2, No. 3, 2012. As of May 7, 2019:
https://www.omicsonline.org/open-access/selected-software-tools-used-for-cbrn-situation-assessment-within-czech-armed-forces-chemical-corps-2167-0374.1000e115.pdf

Prior, Tim, *NATO: Pushing Boundaries for Resilience*, Center for Security Studies, Zürich: ETH Zürich, July 13, 2018. As of April 8, 2019: http://www.css.ethz.ch/en/services/digital-library/articles/article.html/32878ea4-e093-4dbf-a275-5c2f84e25cd6/pdf

Robb, Drew, "Eight Top Threat Intelligence Platforms," eSecurity Planet newsletter, July 18, 2017. As of April 10, 2019: https://www.esecurityplanet.com/products/top-threat-intelligence-companies.html

Robertson, George, "Tackling Terror: NATO's New Mission," speech at the American Enterprise Institute, Washington, D.C., June 20, 2002, June 25, 2002. As of May 7, 2019: https://www.nato.int/docu/speech/2002/s020620a.htm

———, "Launch of NATO CBRN Defense Battalion," remarks, NATO Secretary General, December 1, 2003. As of May 7, 2019: https://2001-2009.state.gov/p/eur/rls/rm/2003/26799.htm

Serena, Chad C., Isaac R. Porche III, Joel B. Predd, Jan Osburg, and Brad Lossing, *Lessons Learned from the Afghan Mission Network*, Santa Monica, Calif.: RAND Corporation, RR-302-A, 2014. As of April 5, 2019: https://www.rand.org/pubs/research_reports/RR302.html

"Smart Defence," topical page, *NATO Review*, undated. As of April 8, 2019: https://www.nato.int/docu/review/topics/en/smart-defence.htm

Strom, Blake E., Andy Applebaum, Douglas P. Miller, Kathryn C. Nickels, Adam G. Pennington, and Cody B. Thomas, *MITRE ATT&CK: Design and Philosophy*, MITRE Corporation, July 2018. As of April 8, 2019: https://www.mitre.org/publications/technical-papers/mitre-attack-design-and-philosophy

Terzuolo, Eric, *NATO and Weapons of Mass Destruction: Regional Alliance, Global Threats*, Abingdon-on-Thames: Routledge, 2006.

Tyson, Ann Scott, "In New NATO, a Division of Military Labor," *Christian Science Monitor*, November 27, 2002. As of May 7, 2019: https://www.csmonitor.com/2002/1127/p02s01-wogi.html

Underwood, Kimberly, "NATO Strengthens Its Cyber Stance," *Cyber Edge*, April 1, 2018. As of April 10, 2019: https://www.afcea.org/content/nato-strengthens-its-cyber-stance

U.S. Department of Homeland Security, "National Cyber Incident Response Plan," December 2016. As of April 10, 2019: https://www.us-cert.gov/sites/default/files/ncirp/National_Cyber_Incident_Response_Plan.pdf

U.S. Joint Chiefs of Staff, *Joint Intelligence*, Joint Publication 2-0, Washington, D.C., October 22, 2013. As of April 8, 2019: http://www.jcs.mil/Portals/36/Documents/Doctrine/pubs/jp2_0.pdf

———, *Cyberspace Operations*, Joint Publication 3-12, Washington, D.C., June 8, 2018. As of April 8, 2019: https://www.jcs.mil/Portals/36/Documents/Doctrine/pubs/jp3_12.pdf?ver=2018-07-16-134954-150

———, *Operations in Chemical, Biological, Radiological, and Nuclear Environments*, Joint Publication 3-11, Washington, D.C., October 29, 2018, II-18. As of May 7, 2019: https://www.jcs.mil/Portals/36/Documents/Doctrine/pubs/jp3_11.pdf?ver=2018-12-07-091639-697

"Washington Summit Communique," North Atlantic Council, Washington, D.C., April 24, 1999. As of May 7, 2019: https://clintonwhitehouse2.archives.gov/WH/New/NATO/statement3.html

Zimmerman, Carson, *Ten Strategies of a World-Class Cybersecurity Operations Center*, MITRE Corporation, Bedford, Mass., 2014.

About the Authors

Lillian Ablon was an information scientist at the RAND Corporation. She conducted research on the intersection of cybersecurity, computer networks, information systems, privacy, commercial technology, and public policy.

Anika Binnendijk is a political scientist at the RAND Corporation, with prior experience at the Office of the Secretary of Defense and State Department Office of Policy Planning. Her research currently focuses on national security decision-making, European defense, gray-zone challenges, and national resilience.

Quentin E. Hodgson is a senior international and defense researcher at the RAND Corporation, focusing on cybersecurity, cyber operations, risk management, and command and control. He has led projects for the Office of the Secretary of Defense, the Department of Homeland Security, and NATO's Allied Command Transformation.

Bilyana Lilly is a Ph.D. student at Pardee RAND Graduate School and an assistant policy researcher at RAND. She specializes in national and transnational security issues in Russia, Europe, and the United States, including cybersecurity, NATO, defense strategy, security cooperation, missile defense, and deterrence.

Sasha Romanosky, Ph.D., is a policy researcher at the RAND Corporation and former cyber policy advisor at the Pentagon in the Office of the Secretary of Defense for Policy. He researches topics in the economics of security and privacy, information policy, applied microeconomics, national security, and law and economics.

David N. Senty is an Adjunct Senior Fellow at the RAND Corporation with a research emphasis on the technologies, concepts, and policies for cyber operations. A retired U.S. Air Force major general, he was the first chief of staff at U.S. Cyber Command. He also is a 33-year veteran of the Central Intelligence Agency, principally as a senior technical operations officer.

Julia A. Thompson is a defense analyst currently researching issues pertaining to the health of the missiles and munitions industrial base for the U.S. Department of Defense. Previous research at RAND has focused on crisis management, South Asian security, and nuclear and conventional deterrence.

About This Perspective

At the June 2016 Ministerial Meeting, the NATO Defence Ministers agreed to recognize cyberspace as an operational domain. That decision was endorsed and reaffirmed at the NATO Summit in Warsaw in July 2016. As part of this effort, NATO directed the development of an implementation roadmap for review at the February 2017 Defence Ministerial Meeting.

NATO's Allied Command Transformation (ACT) requested the RAND Corporation's assistance to provide analysis that would inform the implementation of the roadmap, focusing on identifying lessons learned from national practice; conducting analysis and engagement to develop, refine, and improve material to inform NATO decisionmaking; and providing an independent, objective view on approaches to implement the roadmap.

This Perspective leverages insights from that focused analytic effort and provides additional commentary suitable for a wider audience. In particular, we discuss three viewpoints relevant to this endeavor upon which NATO is embarking, focusing on NATO's past, current, and emerging position in cyberspace.

This research was sponsored by NATO ACT and conducted within the Cyber and Intelligence Policy Center of the RAND National Security Research Division (NSRD). NSRD conducts research and analysis for the Office of the Secretary of Defense, the Joint Staff, the Unified Combatant Commands, the defense agencies, the Navy, the Marine Corps, the U.S. Coast Guard, the U.S. Intelligence Community, allied foreign governments, and foundations.

For more information on the RAND Cyber and Intelligence Policy Center, see www.rand.org/nsrd/ndri/centers/intel.html.

For more information on this publication, visit www.rand.org/t/PE329.