# How is NATO Meeting the Challenge of Cyberspace?

By Jamie Shea

Historians of international relations are familiar with the hinge-year concept when trends that previously had been largely subterranean suddenly crystallize into a clear and immediate danger, forcing policymakers to wake up and take action. When it comes to cyberspace, the past year has certainly smashed any complacency about our ability to anticipate and counter the growing sophistication of cyberattacks. As fast as we have tried to catch up, the speed and global impact of these attacks continue to outrun us. 2016 witnessed the first major attack via the Internet of Things when a DynCorp server in the United States was hacked through video surveillance cameras. We also saw the first attacks driven by artificial intelligence, and increasing evidence of collusion between state intelligence services and organized crime networks.

Yet it is not the much discussed theme of the economic damage inflicted by cyber crime in the past year that has dominated the debate. It is more the use of cyber as an instrument of state policy, political influence, and manipulation. From being a useful tool of espionage and intellectual property theft, cyber intrusions have evolved into a potent instrument of hybrid warfare and outright political vandalism. Ukraine, for example, has been the victim of an unprecedented and systematic campaign of cyber bullying. It has acknowledged up to 2,000 orchestrated cyberattacks since Russia occupied Crimea in March 2014. It has suffered disruption to its election voting system, train and airline on-line booking, ports, electricity grid, and most recently, the massive elimination of tax and financial accounting data through the NotPetya malware. Initially disguised as a ransomware attack similar to the previous WannaCry, a hack that affected more than 200,000 computer networks in 150 countries, it soon became clear that the data encrypted was being destroyed, and that the motive of the attack was not financial gain but rather economic and structural sabotage. Although companies in other countries were also affected by NotPetya, 80 percent of the impact was in Ukraine.[1] Intelligence analysts now agree that NotPetya was a state-driven effort. All of these orchestrated cyber campaigns suggest that Ukraine is being used as a laboratory or proving ground to test a range of cyber weapons and assess their impact, with widespread collateral damage elsewhere accepted as a consequence of doing business; or even as a way to cover tracks.[2]

Given the difficulty of technical attribution and the inability of governments to deter or retaliate against cyberattacks in a manner that demands the attacker's attention but avoids unwanted escalation, NATO has

Dr. Jamie Shea is Deputy Assistant Secretary General for Emerging Security Challenges at NATO. The views expressed are entirely those of the author and should not be construed as an official position of NATO.

had to take a hard look at its preparedness, not only to fend off cyberattacks but also to preserve its political and military freedom of navigation in the cyber domain. The revelation in a recent *Washington Post* article of how the Obama Administration rejected nearly all proposed responses to Russian incursions into the communications of the Democratic National Committee because they were deemed to be ineffective, escalatory, or would compromise long-term U.S. intelligence gathering and prematurely expose U.S. offensive cyber capabilities, caught NATO's attention.[3] There is growing awareness that Russian operational activity built around groups such as APT28 is aimed at inflicting damage to the reputation and cohesiveness of organizations such as NATO.[4] Consequently, reducing the strategic cyber threat to the functionality of governments and societies and making cyberspace more stable and transparent has become as important to international peace and order as nuclear arms control or the conventional balance of power.

The starting point for this effort is the recognition that every future crisis or conflict will have a cyber dimension, and that just as NATO has had to build missile defense and conventional postures into its traditional nuclear-based deterrence strategy, it will need increasingly to incorporate cyber expertise and capabilities as well. This will require not only planning and resources but an important intellectual effort to better understand the precise contribution that cyber capabilities can make to deterrence and defense or indeed crisis resolution, and when military commanders might want to use them in preference to traditional military tools.

Key questions include; is it worth investing more in cyber efforts than conventional equipment in terms of cost-effectiveness? When does it make more sense to invest scarce resources in people skills or better processes rather than upgrading technology? Can the collateral damage of cyber effects be precisely assessed and contained? Will their impact be short-term or long-term, tactical or strategic on the battlefield? Can cyber capabilities be incorporated into existing NATO command and control structures, or do they require more distinct and specialized structures?[5] Most importantly, how can senior Alliance political and military leadership train itself to be as efficient in assessing and responding to a hybrid operation based on cyber as to a crisis involving political, economic, conventional, or nuclear elements; or in the more traditional domains of land, sea, and air?

Many key aspects of cyber crisis management will need to be explored in this discussion: the use of exercises; what kind of intelligence/attribution picture is required; what kind of force generation of cyber effects as part of a broader spectrum of crisis response measures; and how to do cyber messaging to enhance deterrence as well as public support and legitimacy for NATO's actions, especially in an environment where cyber capabilities are shrouded in considerably more secrecy than the usual elements of the diplomatic and military toolbox. In the course of this discussion, it has also become clear that it is difficult to determine appropriate messaging on cyber activity, particularly when it comes to the timing, scope, and utility of offensive options, and that the best approach continues to be to learn the lessons from past attacks and improve defenses.

## Developing the Toolbox

The sense of alarm regarding the evolving cyber threat to Allied nations as well as to NATO itself should not detract from the steps that the Alliance has already taken toward being a more cyber-capable and enabled organization. At the very least, these have considerably enhanced NATO's cyber literacy and defined a framework to take cyber work forward with more systematic political guidance and oversight. NATO declared at its July 2016 Summit in Warsaw, that the Alliance now considers cyberspace as a fifth operational domain (in addition to land,

sea, air, and space). This essentially took NATO from the protection of the internal network (information assurance) to the cyber defense of every military activity (mission assurance).

In order to adjust to this new reality in which cyberspace is not only a new fifth domain of warfare in its own right, but also impacts the four traditional domains of warfare, NATO defense ministers in February 2017 approved a roadmap outlining the steps needed for the Alliance to fully implement the domain concept by 2019. This roadmap provides for a closer relationship between the Supreme Allied Commander Europe (SACEUR) and his Allied Command Operations, and the NATO Communications and Information Agency in The Hague, which is responsible for the daily protection and monitoring of NATO's networks in peacetime, and for the security and acquisition of NATO's information technology. This will ensure a smooth transition from civilian to military responsibility in a crisis situation. NATO is also updating its operational plans to better incorporate and prioritize cyber defense and to have a clearer sense of related requirements during operations.

Clearly, cyberspace has accelerated the speed at which crises can unfold, leading to the requirement for much better and earlier situational awareness and responsive decision-making. Operating "at the speed of relevance" has become the new buzz phrase. Accordingly, NATO's military commanders are working on a set of crisis response measures that will allow them to initiate forward scanning of networks, active defense measures, and the activation of a back-up NATO Computer Incident Response Capability (NCIRC). At the same time, a real effort must be made to understand how NATO's potential adversaries (Russia for example) are conceptualizing cyber in their doctrine, and what lessons they are learning from their ongoing covert cyber operations to develop this doctrine and adapt their cyber capabilities to a spectrum of projected missions. If we cannot stand still, then we must assume that they are not standing still either.

As NATO moves toward cyberspace as a domain, it needs to practice better to cope with offensive cyber as part of an access and area denial strategy, and rehearse more realistically these scenarios in its crisis management exercises and also in its Trident series of military exercises. This means better aligning cyber work with the Alliance's enhanced forward presence in Poland and the Baltic States, and its associated graduated response plans, particularly when it comes to SACEUR's ability to exercise full control of his area of responsibility and get reinforcements into place quickly. It also means a better coordination of effort across the NATO Command structure. Already SACEUR has set up a Cyber Division at Allied Command Operations, in order to better identify requirements and ensure that NATO's capability packages to common fund its acquisitions reflect the cyber dimension.

In this respect, NATO will need to meet the challenge of accelerating its upgrades to its information technology and to the NCIRC. NATO must move from a culture where capabilities are acquired in big chunks or platforms and at intervals of ten or fifteen years, to one in which information technology can be constantly upgraded in an evolutionary way, with incremental investments on a more frequent basis. The analogy is not going from an old car to a new one but constantly modifying the car so that it becomes impossible to determine when the old car has disappeared and the new one has taken its place. Otherwise there is a danger of technology becoming obsolete every two to three years, and that NATO's acquisitions process will constantly leave NATO behind the technological curve. If NATO's current capability packages are overloaded with too many different elements, and take an average of 16 years to implement, this challenge will not be met. Clearly, to improve on cyber delivery, political guidance, which is next due in

June 2019, has to be much more expansive and detailed on operational cyber requirements and capabilities than we have seen in the past.

Finally, another requirement associated with making cyberspace an operational domain is that NATO will need to learn more from its Allies who have already moved in this direction, such as the United States, the United Kingdom, France, and the Netherlands; how their models are working, and how they are intending to use cyber effects as part of their military operations. Some Allies, like Estonia and France, are putting the emphasis on a reservist force of civilian cyber specialists and cyber as a fourth army with a light, agile structure rather than as part of a classic, top heavy military chain of command. Should cyber follow a similar model in NATO at a time when the Alliance is refashioning its command structure to support corps level, heavy armoured and combined arms operations in Eastern Europe? NATO's political guidance for these issues is all the more important as NATO will not develop offensive cyber capabilities and would therefore need to rely upon national capabilities (subject to political approval by NATO overall) in instances where NATO military commanders believe that a cyber effect rather than the use of a conventional weapon is the best way of producing a desired military outcome. The U.K. Defense Minister has already offered U.K. national cyber capabilities to NATO on a voluntary basis, and other Allies may well make similar commitments in the near future. In the meantime, NATO's Cyber Defence Committee will work on a set of agreed principles for how a mechanism could function within NATO to give Allies effective political oversight for these national contributions used in the collective name of the Alliance. A question is whether these national cyber contributions could be used in a pre-conflict, hybrid warfare scenario, or only once a full-scale kinetic conflict has broken out.

The success of cyber as a domain ultimately depends on a two-way process. NATO must optimize the ability of cyber instruments to support classic military operations on land, sea, or in the air, but also ensure that the future NATO organizational construct and command structure have the requisite skilled personnel, rules of engagement, operational planning, and rapid access to capabilities to support advanced cyber operations. Additionally, as the Alliance deploys advanced capabilities, such as Global Hawk observation drones, joint intelligence surveillance and reconnaissance sensors, integrated air and missile defense, and its new air command and control system, these will need to be hard proofed against cyberattacks. Therefore, cybersecurity needs to be factored into all acquisition programs and in the systems design and development, rather than as an afterthought.

*Cybersecurity needs to be factored into all acquisition programs and in the systems design and development, rather than as an afterthought.*

## The Cyber Defense Pledge

The second major initiative of NATO's 2016 Warsaw Summit was to adopt a Cyber Defence Pledge. Readers of this article will be familiar with an earlier Pledge from NATO's previous Summit in Wales in 2014 for each Ally to spend a minimum of 2 percent of its GDP on defense. The Cyber Defence Pledge commits Allies to spend at least a portion of this extra investment on improving national cyber defenses, even if there is no specified minimum amount. Effective cyber defense depends upon building a community of trust in which there are no weak links in the chain.

Otherwise, the more cyber capable Allies might be reluctant to share sensitive information and expertise with Allies who have not brought their national cyber defenses up to a minimum level of security. As NATO depends in nearly every area on national capabilities rather than commonly owned assets (AWACS aircraft being the exception), its ability to operate in the cyber domain depends upon its success in setting more ambitious capability targets for its member states, and to encourage them to plug identified gaps. By inducing the Allies to perform more regular assessments of their levels of preparedness, the Cyber Defence Pledge should make this effort easier in the future.

Allies have carried out self-assessments of cyber defense hygiene by reporting on seven capability areas—from strategy, organization, processes and procedures, threat intelligence, and partnerships, to capabilities, and investments. They have been asked to benchmark these assessments on a scale from advanced to relative beginner. National responses will allow the NATO staff to develop more precise and relevant metrics, as well as to form a more reliable common baseline of overall NATO capabilities. In turn, this greater transparency will help the NATO staff to identify gaps and prioritize requirements. On this basis, the well-known NATO Defence Planning Process, which has already incorporated a set of basic cyber capability targets for each NATO member state, will be able to suggest more ambitious targets better adapted to the needs of individual states in the future. The peer pressure that greater transparency should generate will incentivize Allies to meet their assigned targets and to stimulate bilateral assistance. An initial report on the first stage of the Cyber Defence Pledge was provided to NATO Defence Ministers last June. The good news is that for the 2017–19 cycle, all the capability targets set by NATO's Defence Planning Process have been apportioned and accepted by the Allies—for the first time, it must be said.

## Building a True Cyber Defense Community

Beyond these two flagship initiatives of the 2016 Warsaw Summit, a good portion of NATO's effort to step up its game in cyber defense, is to enhance its ability as a platform to assist the Allies across a whole spectrum of cyber defense needs. For instance, a new memorandum of understanding (MOU) between NATO Headquarters (HQ) and individual Allies has been offered to improve intelligence sharing, crisis management, and lessons learned from cyberattacks. Already 22 of the 29 Allies have signed this new MOU. NATO has established a new intelligence division with a strong cyber threat intelligence function, which should incentivize Allies to provide more early warning and advance notice of cyberattacks or malware and not only lessons learned and post–incident information. Enhanced intelligence sharing among Allies will not only help to parry cyberattacks or to limit their damage but also to build over time a much more detailed and comprehensive picture of hacker groups, proxies, methodologies, and attribution techniques.[6]

One of NATO's most useful contributions to its member states is in the organization of trainings and exercises to improve the skill set not only of the 200 operators in the NCIRC and the NATO command structure, but also those of national cyber defense teams. The annual *Cyber Coalition* exercise now attracts more than seven hundred participants, and the *Locked Shields* exercise, involving 900 participants this year and won by the Czech Republic, is recognized as one of the most demanding and intensive Red Team–Blue Team exercises. This year it exercised the cyber vulnerabilities of drones, power grids, and programmable logic controllers. A strategic storyline was used to put the technical exercises in a contemporary political context. Both of these exercises take place at the NATO Cooperative Cyber Defence Centre of Excellence in Estonia and have


Operation *Locked Shields 2017* arranged by the NATO Cooperative Defence Center for Excellence. (NATO Cooperative Defence Center for Excellence)

the use of the recently upgraded cyber defense range, which Estonia has offered to NATO.

Beyond exercising, NATO must train civilian and military personnel on a regular basis in cyber defense concepts and basic procedures, as well as organize courses on cyber hygiene for end-users across the entire NATO enterprise. A cyber security scorecard developed by the United States can help to visualize and manage basic cyber hygiene in real-time, focusing on the protection of sensitive data, information management, and cryptology.[7] Portugal has taken the lead in the Alliance on this type of training and education and will soon acquire the NATO Communications and Information School, which is being transferred from Italy to Portugal. The plan is to augment this school with a Cyber Defence Academy, which will both serve as a training center as well as a forum for a permanent interchange among NATO personnel, academia, and industry, with a cyber laboratory to facilitate innovation and experimentation. At the same time, NATO is assisting those Allies who have agreed to lead smart defense projects in cyber defense. In addition to Portugal's project on education and training, Belgium has successfully led a group that has developed a malware information sharing platform, which has not only been implemented among Allies but also between NATO and the European Union. A variant of this is also being used to facilitate the exchange of information between NATO and industry, with the possibility of more open as well as more confidential platforms according to the level of certified access and the sensitivity of the information being shared. A third cyber defense project focuses on situational awareness and incident coordination, including an operations and maintenance contract. The system has been successfully implemented by the Netherlands and Romania. All in all, 25 Allies and six Partners participate in smart defense projects.

Moreover, NATO now has a Cyber Defence Committee. This has been instrumental in persuading Allies to send cyber experts to NATO HQ on a permanent basis and to improve links between HQ and important national centers, such as Cyber Command and the National Security Agency in the United States, or its counterpart, the Government Communications Headquarters (GCHQ) in the United Kingdom. The Committee also serves as a focal point for industry and the NATO military command structure and NATO agencies to provide inputs into the policymaking and decisionmaking levels of NATO. New models for priority items like advanced technical measures, cyber resilience and robustness constructs, risk management models, and cyber security standards can be presented and validated by the Committee, which also has responsibility for monitoring NATO's Cyber Defence Action Plan implementation, updating the overall policy, and reporting in detail on progress to every meeting of NATO Defence Ministers. The Committee is the essential link between the technical operating level and the policymaking level, without which progress would be ad hoc and uncoordinated. A Cyber Defence Management Board within NATO HQ brings all the relevant actors together to assess and respond to specific cyberattacks and other incidents and to regularly monitor threat intelligence and early warning indicators. All these various activities are helping to make NATO the natural platform for setting the level of ambition and defining a common set of standards and requirements for its member states in cyber defense.

## It Takes a Network to Defeat a Network

Finally, if NATO is to raise its game, it must have even stronger partnerships. Collaboration is the mantra in the cyber domain. Successful cyber defense depends upon being able to bring a much larger cast of actors around the same table than in the past, when we were dealing with much more limited and largely uniform circles to handle things like nuclear deterrence or missile defense. Yet

collaboration even if necessary is not automatic. It requires full-time attention and resources to create and sustain relationships, as well as incentives so that over time partners believe they are getting as much out of the relationship as they are being asked to put in. Partnership should not become an end in itself, with networking for the sake of networking. Resources are limited so decisions must be made regarding which partners have to be prioritized and in which stages. Moreover, every organization must determine how many of its essential functions it needs to provide in-house and which ones it cannot manage by itself and can more cost-effectively outsource to outside entities. In sum, partnership needs as much of a strategic approach as any other aspect of cyber defense and must be driven from the top.

Toward this purpose, NATO has reached out to industry and formed a NATO Industry Cyber Partnership. Thus far, the NATO Communications and Information Agency has concluded twelve individual partnership arrangements with industry to share threat intelligence and early warning indicators. This has proved its worth in facilitating real-time information-sharing and rapid assessment of the recent WannaCry and NotPetya attacks. An improved series of NATO industry workshops, such as the annual NATO Information Assurance Symposium in Belgium and a series of threat vector workshops, are bringing industry and NATO together to discuss innovation, improving procurement and acquisition, and threat intelligence. Another area of interest for NATO is industry's experience of resource prioritization: when is it best to spend limited budgets on personnel and skills vis-à-vis technology upgrades or improved processes? This engagement with industry is also designed to help NATO better understand which security products are out there on the market which NATO could better exploit while also helping industry to see where NATO's procurement is likely to be heading in the future. A key concept of innovation is "fail fast," as effective cyber defense would be hampered if it takes too long to determine which innovative products will work and which will ultimately under-perform.

The NATO Industry Cyber Partnership can also improve supply chain management and stimulate diversity on the supply side. An information exchange has been set up at the NATO Communications and Information Agency that has been conducting pilot projects to see how we can better link up with academic research and small and medium-sized companies that are often in the forefront of innovation but which have often been reluctant to engage NATO directly or uncertain where to plug in to the NATO bureaucracy.[8] Hopefully, in time this innovation exchange will benefit from NATO common funding to organize trials, demonstrations, and simulations of NATO networks to test the usefulness of various products in a real-time environment. At all events, Allies are now sharing more information on their trusted industries, making it easier for an Ally in one country experiencing a cyber disruption, for instance on a power station or water facility, to identify in another NATO country a company that has the expertise to offer a rapid response with certified technology and supply chain security.

At the same time, NATO is building stronger relationships with other countries that have concluded a formal partnership arrangement with the Alliance. A political framework arrangement on cyber defense was recently agreed with Finland. A trust fund for the provision of cyber defense equipment and analytical and forensic capabilities is in operation with Ukraine. Moreover, NATO has been helping countries such as Jordan, Moldova, and Georgia with cyber defense organization at the national level, doctrine, and training. Partners are increasingly joining the Cooperative Cyber Defence Centre of Excellence in Tallinn (Sweden being the latest) or sending staff or observers there. In Brussels, NATO and the European Union (EU) are now coming together more closely in the cyber defense field. A technical arrangement on

the sharing of non-classified information between NCIRC and the EU Computer Emergency Response Team (CERT–EU), which certifies that a company has fulfilled the legislative criteria required in each country, has been in operation for more than a year. The recent action plan to implement the NATO–EU Joint Declaration provides for more NATO–EU interaction; for instance in sharing information on operational planning for cyber defense during military missions, harmonizing training requirements, cooperating more on research and development, and standards between the European Defence Agency and NATO's Allied Command Transformation, and more mutual participation in each other's training and exercises, such as NATO's CMX, Cyber Coalition, and the EU's Cyber Europe. The current Estonian presidency of the EU has made information technology security its top priority. This should help NATO and the EU to hold more table top exercises and do joint strategic thinking on the future of the internet and how to promote better governance and norms for cyberspace, particularly at a time when the GGE (Group of Governmental Experts) process in the United Nations has stalled.

involved, for better and for worse. Resources must be spread over a far greater number of functions and applied much more selectively than in a conventional capability program if a cyber construct is to operate successfully. Many more countries, groups, and levels of threat and risk have to be monitored and assessed simultaneously than is the case with classic conventional or nuclear adversaries. There is the problem of attribution and as the recent hacking during the U.S. elections has shown, still a good deal of uncertainty as to when a cyberattack, which does not necessarily kill people or destroy anything physical, can really be considered an act of aggression justifying retaliation. Whereas we have a good idea how to deter a nuclear or conventional attack, to deal with crises in the traditional domains, to employ arms control or confidence-building arrangements, we still do not have a good idea of how to deter or respond to major cyberattacks, even when they are clearly designed to undermine our governments or our political processes. We can try to privately warn the suspected perpetrators; we can impose sanctions or indict certain individuals or organizations, as the United States has done in response to the Yahoo

*Whereas we have a good idea how to deter a nuclear or conventional attack, to deal with crises in the traditional domains, to employ arms control or confidence-building arrangements, we still do not have a good idea of how to deter or respond to major cyberattacks, even when they are clearly designed to undermine our governments or our political processes.*

## Working at the Top but also at the Bottom

Cyber differs from the other domains of conflict: the pace of innovation is much faster, the technology is much more decentralized, and many more actors are

attack and the 2016 election interference; but as long as an adversary judges the gains to significantly outweigh the risks, then deterrence is not going to work.[9] So we will have to think more strategically about increasing the penalties and limiting the

gains as we go forward. At the same time, cyber is problematic because as we contemplate the more strategic use of cyber, we still have to deal with the more conventional problems we have been confronting for the past 20 years or so.

In the first quarter of 2016, there was a 250 percent increase in the number of phishing sites and related email traffic vis-à-vis the final quarter of 2015.[10] The most recent McAfee Labs threats report warns that for every ten phishing emails sent by attackers, at least one will be successful. McAfee presented ten real emails to more than 19,000 people from across the globe and asked them to identify whether they were dangerous or legitimate. It found that 80 percent incorrectly identified at least one phishing email.[11] According to Verizon, 30 percent of phishing messages are opened and around 12 percent allow the attack to succeed by clicking the malicious attachment or link.[12] In 2016, there was a 400 percent spike in ransomware families with 15 new ones discovered on average every month.[13] Meanwhile, denial-of-service attacks are becoming larger and the average pay out from business email compromises is now running at $140,000.[14] These examples demonstrate that as we grapple with the new threats and challenges, we are still struggling to get the basics right, and are still vulnerable to the oldest and simplest intrusion techniques.

Accordingly, the cyber domain will require NATO to increasingly work top down on anticipating the strategic trends and adjusting policy and doctrine more quickly, while working bottom up at improving basic cyber hygiene to lower its attack surface and reduce the scope for own goals due to basic human error. What was after all so depressing about the manipulation of the U.S. elections was the fact that so much damage could be inflicted through the simple expedient of a miscommunication between a senior Clinton campaign official, John Podesta, and an IT specialist regarding whether a suspicious email was real or fake. There is a lesson here for all of us; that we will never have effective cyber defense if we raise our own game but fail to raise that of all of our colleagues and partners across the whole enterprise at the same time. Often policy-making falls into periods of decision and periods of implementation, but in reality we need to learn better to do these things simultaneously—learning to transform the plane while we are flying it—if we are to keep pace, let alone ultimately master the evolving cyber threat. PRISM

## *Notes*

[1] For instance, the Danish shipping company Maersk had its container traffic paralyzed around the world losing US$300 million and one UK company, Reckitt Benckiser, suffered £120 million in losses.

[2] For instance, Russia has used WannaCry and NotPetya to claim that it is also the victim of cyberattacks, as some of its own ministries and companies such as Rosneft have been impacted.

[3] Greg Miller, Ellen Nakashima, and Adam Entopus, "Obama's Secret Struggle to Punish Russia for Putin's Election Assault," *Washington Post*, June 23, 2017.

[4] Matt Burgess, "Exposed: how one of Russia's most sophisticated hacking groups operates," *Wired*, January 11, 2017.

[5] France, for instance, has established the post of ComCyber to the Minister of Defense.

[6] A closer relationship with the EU's Europol agency and its Cyber Crime Centre would be useful here, given Europol's database on criminal forensics.

[7] United States Department of Defense, "Improving Cyber Basics—DoD Cyber Discipline Implementation Plan and DoD Cyber Scorecard," December 2016. Available at < http://dodcio.defense.gov/Portals/0/Documents/Cyber/CNDSP%20Plain%20Language%20Overview%20-%20DISTRO.pdf?ver=2017-01-31-125734-897>.

[8] In Europe, 70 percent of the market.

[9] United States Department of Justice, "U.S. Charges Russian FSB Officers and Their Criminal Conspirators for Hacking Yahoo and Millions of Email Accounts," March 15, 2017.

[10] Anti-Phishing Working Group (APWG), "Phishing Activity Trends Report: 1st Quarter 2016," May 23, 2016.
[11] McAfee Press Release, "97% of People Globally Unable to Correctly Identify Phishing Emails," May 12, 2015.
[12] Verizon, *Data Breach Investigations Report*, 2016.
[13] Trend Micro, *The Next Tier - Trend Micro Security Predictions for 2017*, December 2016.
[14] Ibid.

## *Photos*

Page 18: Balic servers data center. From Wikipedia, available at <https://fr.wikipedia.org/wiki/Fichier:BalticServers_data_center.jpg>. Licensed under Creative Commons Attribution-Share Alike 3.0 <https://creativecommons.org/licenses/by-sa/3.0/>. Photo unaltered.