NATO: Stepping up its game in cyber defence

Received (in revised form): 10th May, 2017

Jamie Shea

is NATO Deputy Assistant Secretary General for Emerging Security Challenges. He has been working with NATO since 1980. Positions included Director of Policy Planning in the Private Office of the Secretary General, Deputy Assistant Secretary General for External Relations, Public Diplomacy Division, Director of Information and Press, Spokesman of NATO and Deputy Director of Information and Press, Deputy Head and Senior Planning Officer in the Policy Planning and Multilateral Affairs Section of the Political Directorate as well as Assistant to the Secretary General of NATO for Special Projects. Outside NATO, he is involved with several prominent academic institutions. He is a professor at the Collège d'Europe, Bruges, visiting lecturer in the Practice of Diplomacy, University of Sussex, Associate Professor of International Relations at the American University, Washington DC, where he also holds the position of director of the Brussels Overseas Study Programme. He also lectures at the Brussels School of International Studies at the University of Kent and at the Security and Strategy Institute of the University of Exeter, where he is an honorary fellow. He is also a senior transatlantic fellow of the German Marshall Fund of the United States and a senior fellow at the London School of Economics, where he teaches a course on crisis management and political communication. He is a regular lecturer and conference speaker on NATO and European security affairs and on public diplomacy, political communication and many other areas of contemporary international relations. He holds a DPhil in modern history from Oxford University (Lincoln College), 1981. Among his many associations and memberships, he is a member of the Advisory Board, Security and Defence Programmes at Chatham House, a member of the Policy Council at the World Economic Forum in Geneva and founder and member of the Board, Security and Defence Agenda Brussels and Friends of Europe. He serves on the Board of the Danish Defence College, Copenhagen, and the Académie Diplomatique Internationale in Paris. He is a recipient of the Golden Eagle medal of the Republic of Albania and the Linden medal of the Czech Republic. He was European Communicator of the Year in 1999 and in 2016 was awarded the International Prize for Human Rights of the AAB University in Kosovo.

Deputy Assistant Secretary General, NATO International Staff, 1110 Brussels, Belgium
E-mail: shea.jamie@hq.nato.int

Abstract Events in 2016 significantly raised the importance of cyberattacks, not just to NATO governments but to societies as well. The interference of Russia in the US election campaign, the first major cyberattack through the Internet of Things, the disruption of the Ukrainian energy grid and the publicity given to the greater use of cyber instruments against ISIL or the North Korean missile programme all served to increase public awareness of the multiplicity of the cyberthreat — whether for intelligence gathering, hybrid warfare operations, disruption or even outright destruction, not forgetting in the process the more traditional understanding of cyber as a growing domain of criminal activity. Against this background, NATO has had to raise its game in improving its own cyber defences. This paper outlines the various approaches the Alliance has taken and covers, in particular, NATO's Cyber Defence Pledge to improve the investments, capability development and internal coordination of its member states; NATO's recognition of cyber as an operational domain and what this means for NATO's ability to conduct its missions in a cyber-contested military environment; and finally what NATO is doing to further assist its member states to develop their own capabilities by facilitating education and training, operational exercises, smart defence projects and engagement with industry through the NATO cyber industry partnership. The paper is intended to give a sense to the reader of where NATO is going and is likely to go in the future in making cyber defence part of its core collective defence mission.

KEYWORDS: cyber defence, hybrid warfare, resilience, civil–military relations

Policy making normally comes in two forms. First there is a period of reflection and consultation in order to prepare new initiatives or to update existing policy documents, to bring them into line with new threats. This, however, needs to be followed by a period of implementation and turning initiatives into the reality of hard-core capabilities and organisational change. Initiatives that are not followed up in practice are as unhelpful as random action which is not guided by any notion of strategy or goals to be achieved, or any ability to assess periodically whether a policy is on track or not.

The year 2016 was very much one of policy making and decisions for NATO in the field of cyber defence. In many ways, 2016 was also a watershed year, when cyber defence was no longer purely a question of protecting networks against a growing and more sophisticated spectrum of cyberattacks but instead became an issue of the integrity of democratic institutions in NATO countries. The abuse of cyberspace became a means not just to acquire or manipulate data, or interfere with the running of a particular network, but to influence political outcomes and even exert outright political coercion and intimidation.

FROM CYBERATTACKS TO HYBRID WARFARE

Great publicity surrounded Russia's penetration of the networks of the Democratic National Committee in the United States and its use of extracted e-mail information to discredit the election campaign of Hillary Clinton and the Democratic Party. It was not just the success of the attack that was striking but the fact that the Russian Intelligence Service tried to access as many as 128 private e-mail accounts of the Clinton campaign and only needed ultimately to access two in order to be able to extract sufficient data to achieve — courtesy of WikiLeaks — a devastating impact. In the past, force had to be used to change a government or regime from outside. Could this now be achieved by a cyber-facilitated information operation? The United States election campaign was only the tip of the iceberg, as there were many other attacks, for instance against the German Bundestag, the parliament in Austria, the presidential election campaign of Emmanuel Macron in France, or the Prime Minister's Office in the Netherlands, designed for the same purpose of gaining leverage over political processes or destabilising candidates in close-fought election campaigns. States which hitherto had been rather discreet about their role in these cyberattacks made less of an effort to deny them and groups such as APT28 and APT29 in Russia, commonly known as Fancy Bear and Cozy Bear, achieved great public notoriety. Nowadays, any form of political dispute seems automatically to lead to a series of cyberattacks, both as an expression of anger as well as a more systematic attempt to undermine an adversary by gathering potentially compromising information. The leak of data from the World Doping Agency and attempts to hack into the testing laboratories at the Rio Olympic Games revealed that this type of revenge attack extends as much to the world of sport as of politics — indeed potentially to anywhere where a score needs to be settled.

Yet 2016 marked a watershed in other ways too. The leak of the Panama Papers destabilised the political situation in Iceland and put many well-known politicians under pressure. The heist of the Bangladesh National Bank led to a loss of US$86m, a figure that would have been far worse had the intrusion not been discovered so quickly. This led to questions about the security of the SWIFT international banking system. A leak of data on a massive scale came when Yahoo acknowledged that the accounts of 500m of its customers had been compromised in 2014, probably the largest compromise to have happened thus far. Iran,

according to media reports, came very close to disrupting a dam in the north-east United States by hacking into its industrial control system. The FBI versus Apple dispute over the efforts of the US authorities to gain access to the iPhone of a terrorist showed that even advanced encryption can still be overcome when security institutions really need to gain access to someone's private data. The more recent publication by WikiLeaks of over 8,000 classified CIA communications has drawn further public attention to the attempts by intelligence services to bypass the encryption on popular messaging apps, such as WhatsApp, Telegram and Signal, even if it is not clear if these attempts were successful.

In 2016, we also experienced the first major attack on the Internet of Things, when the servers of DYN Corporation were disrupted through the hacking of video surveillance cameras and webcams, which meant that hundreds of thousands of people in the north-east United States could not access their social media or the websites of media companies like CNN or the *New York Times*. Also in 2016, some worrying new developments came to light. Terrorist organisations such as ISIL and Al Qaeda are turning more and more to cyber hacks to steal money to finance their operations, as their traditional sources of finance begin to dry up. Finally, we also saw the first signs of automated attacks facilitated by artificial intelligence and machine-to-machine learning.

In sum, 2016 was the year when the cyberthreat stopped being a concern primarily for individual entities, such as banks, critical infrastructure providers or hospitals worried about losing data, to become an instrument of hybrid warfare, where the state and society are virtually under permanent attack. Back in 2014, NATO had already declared that a cyberattack above a certain threshold could be considered an armed attack that could trigger the Article 5 Collective Defence clause of the NATO Treaty. At the time this still seemed a hypothetical or even distant prospect. Yet as the new momentum of cyberattacks demonstrates how difficult it is to deter this type of activity, and states on the receiving end begin to feel more insecure and off balance, the prospect of declaring a cyberattack an armed attack and calling for a collective response beyond merely diplomatic protest becomes ever more likely.

MOVING FROM THE TACTICAL TO THE STRATEGIC

It was against this background that NATO had to raise its game in cyber defence. The first response was to declare, at the Alliance's Summit in Warsaw in July 2016, that NATO now considers cyberspace as an operational domain. This means in essence that NATO has decided to shift the focus from information assurance to mission assurance — or, in other words, from a focus on protecting its own internal networks to a focus on the cyber defence of every military activity that it carries out. This shift of emphasis is based on a recognition that cyberthreats will be present at all three stages of NATO's engagement: first in a pre-crisis situation, where the Alliance can anticipate a stepped-up momentum of espionage operations, attempts to penetrate its networks and more robust disinformation campaigns and psychological operations to undermine support for NATO's decisions through the manipulation of data and the planting of fake news. The recent attempts to fabricate stories accusing German soldiers in Lithuania of rape or of conducting psychological operations against the local population are a case in point. The second phase is the crisis itself, when cyberattacks could be used to interfere with NATO's command and control or disrupt its reinforcement activities in Central and Eastern Europe or to carry out sabotage operations on critical infrastructure, such as air traffic control, ports, airfields and pipelines, as well as to deny access to alternative servers and networks. The third

Figure 1: NATO leaders took important decisions at their Summit in Warsaw in July 2016

stage is outright conflict where NATO has to adapt to the need to operate in a cyber-depleted environment where we might not have full access to our networks all the time and would need to rapidly improvise back-up and alternative solutions to achieve minimum functionality. We might also experience attempts to interfere with military systems, such as drones, satellites, air defence and missile defence.

In order to adjust to this new reality in which cyber is not only a new fifth domain of warfare in its own right, but is also impacting on the four traditional domains of warfare (air, land, sea and space), NATO's defence ministers meeting last February approved a roadmap outlining the steps that need to be taken so that the Alliance can fully implement the domain concept by 2019. This roadmap provides for a closer relationship between the Supreme Allied Commander Europe 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 is in order to ensure a smooth transition from civilian to military responsibility in a crisis situation. NATO is also updating its operational plans to better incorporate and prioritise cyber defence and to have a clearer sense of cyber defence requirements during operations — for instance, which cyber effects would need to be generated at an early stage and how can the cyber aspect be better reflected in graduated response plans and crisis response measures, which the NATO Council would authorise SACEUR to implement? 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 taking. 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 would allow them to initiate forward scanning of networks, active defence measures and the activation of a back-up NATO Computer Incident Response Capability (NCIRC).

So, as NATO moves towards cyber as a domain, it needs to practise better for these scenarios in its crisis management exercises and also in its Trident series of military exercises, so that we can cope effectively with this new reality. This 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 speeding up its upgrades to its information technology and to the NATO Computer Incident Response Capability, which is responsible for the daily defence of NATO's networks. We must move from a culture where capabilities are acquired in big chunks or platforms and at intervals of every ten or 15 years to one in which information technology can be constantly upgraded in an evolutionary way and with smaller amounts of investment but 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 on average 16 years to implement, this is a challenge that will not be met.

Finally, another issue associated with making cyber an operational domain is that NATO will need to learn more from its allies who have already moved in this direction, such as the US, the UK, France and the Netherlands, how their models are working and how they are using cyber effects as part of their military operations. This is all the more important as NATO will not develop offensive cyber capabilities and would therefore need to be able to rely upon voluntary 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 success of cyber as a domain ultimately depends on a two-way process. We have to optimise the ability of cyber instruments to support classic military operations, but also ensure that the future NATO organisational construct and command structures 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 defence and its new air command and control system, these will need to be hard-proofed against cyberattacks. Therefore cyber security needs to be factored into all acquisition programmes and in the systems design and development, rather than as an afterthought.

MORE TRANSPARENCY AND BETTER-TARGETED INVESTMENTS

The second major initiative of NATO's Warsaw Summit was to adopt a Cyber Defence Pledge. Readers of this paper 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 per cent of its GDP on defence. The Cyber Defence Pledge commits allies to spend at least a portion of this extra investment on improving national cyber defences, even if there is no specified minimum amount. Effective cyber defence depends upon building a community of trust in which there are no weak links in the chain. Otherwise, the cyber-capable allies might be reluctant to share sensitive information and expertise with allies who have not brought their national cyber defences up to a

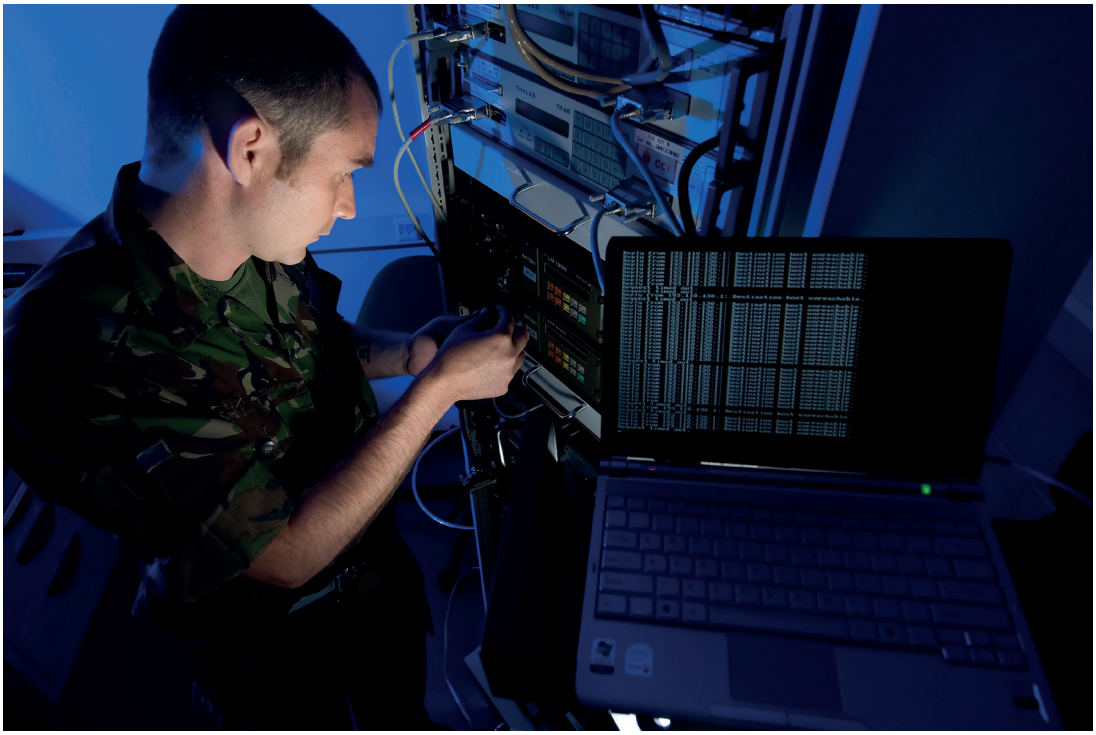

Figure 2: The rapidly evolving nature of the cyber threat underscores the importance of investing not only in the latest cutting-edge technologies, but also in sharpening skills.

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 their cyber defence hygiene by reporting on seven capability areas — from strategy, organisation, processes and procedures, threat intelligence, partnerships to capabilities and investments. They have been asked to benchmark these assessments according to four levels — from advanced to relative beginner. The 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 prioritise 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 and ones more adapted to the needs of individual states in the future. The peer pressure that greater transparency should generate will incentivise allies to meet their assigned targets and to stimulate bilateral assistance. The aim is to provide an initial report on the first stage of the cyber defence pledge to NATO defence ministers in June 2017.

BUILDING A TRUE CYBER DEFENCE COMMUNITY

Beyond these two flagship initiatives of the Warsaw Summit, a good portion of NATO's

effort to step up its game in cyber defence is to enhance its ability as a platform to assist the allies across a whole spectrum of cyber defence needs. For instance, a new Memorandum of Understanding (MOU) has been offered to allies to improve intelligence sharing, crisis management and lessons learned from cyberattacks between NATO HQ and individual allies. Already 21 of the 28 member states have signed this new MOU. NATO has set up a new Intelligence Division with a strong cyberthreat intelligence function, which should incentivise allies to provide more early warning and advance notice of cyberattacks or malware and not only lessons learned and post-incident information several weeks after attacks have taken place. Enhanced intelligence sharing among allies will not only help to parry cyberattacks or to limit the damage but also to build over time a much more detailed and comprehensive picture of hacker groups, proxies, methodologies and attribution techniques. One of NATO's most useful contributions to its member states is in the organisation of training and exercises to improve the skill set not only of the 200 operators in NCIRC and the NATO command structure but also national cyber defence teams. The annual Cyber Coalition exercise now attracts over four hundred participants and the Locked Shields exercise is recognised as one of the most demanding and intensive Red Team–Blue Team exercises. Both of these take place at the NATO Cooperative Cyber Defence Centre of Excellence in Estonia and have the use of the recently upgraded cyber defence range, which Estonia has offered to NATO. Beyond exercising, there is a need to train NATO civilian and military personnel on a regular basis in cyber defence concepts and basic procedures, as well as to organise courses on cyber hygiene for the end-users across the entire NATO enterprise. 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 Latina in Italy to Oeiras in Portugal. The plan is to augment this school with a Cyber Defence Academy, which will serve both as a training centre and as a forum for a permanent interchange between NATO personnel and 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 Defence projects in cyber defence. 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 and with the possibility of more open and more confidential platforms according to the level of certified access and the sensitivity of the information being shared. A third cyber defence 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, 21 allies and four Partners participate in Smart Defence projects.

Moreover, NATO now has its own 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 NATO Headquarters and important national centres, such as Cyber Command within the NSA in the United States, or GCHQ in the UK. The committee also serves as a focal point for industry and the NATO military command structure and NATO agencies to provide inputs into the policy-making and decision-making 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. In other words, the committee is the essential link between the technical operating level and the policy-making level, without which progress would be ad-hoc and uncoordinated. A Cyber Defence Management Board within NATO Headquarters 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 defence.

ONLY STRONG TOGETHER

Finally, if NATO is to raise its game, we need to have even stronger partnerships. Collaboration is of course the mantra in the cyber domain, as we all know that successful cyber defence depends upon being able to bring a much larger cast of actors around the same table than was ever the case in the past, when we were dealing with much more limited and largely uniform circles to handle things like nuclear deterrence or missile defence. Yet collaboration, even if necessary, is not automatic. It requires full-time attention and resources to create and sustain relationships. It also requires 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 taken on which partners have to be prioritised and in which stages. Moreover, every organisation should 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 subcontracted to outside entities. In sum, partnership needs as much of a strategic approach as any other aspect of cyber defence and needs to be driven from the top.

Against this background, NATO has reached out first and foremost to industry and formed a NATO Cyber Industry Partnership. Thus far, the NATO Communications and Information Agency has concluded 12 individual industry arrangements to share threat intelligence and early warning indicators. An improved series of NATO industry workshops, such as the annual NATO Information Assurance Symposium in Mons and a series of threat vector workshops, is 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 prioritisation — in other words, when is it best to spend limited budgets on personnel and skills *vis-à-vis* technology upgrades or improved processes? This earlier 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. It can also improve supply chain management and stimulate diversity on the supply side. An innovation exchange has been set up at the NATO Communications and Information Agency and this 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 have often been reluctant to engage with NATO directly or uncertain where to plug into the NATO bureaucracy. Hopefully in time this innovation exchange will be able to benefit from NATO common funding to organise

trials and demonstrations and use 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, which is 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 also building stronger relationships with other countries that have concluded a formal partnership arrangement with the Alliance. A technical arrangement on cyber defence was recently agreed with Finland. A trust fund for the provision of cyber defence 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 defence organisation at the national level and doctrine and training. Partners are increasingly joining the Cooperative Cyber Defence Centre of Excellence in Tallinn or sending staff or observers there. In Brussels, NATO and the European Union are now coming much closer together in the cyber defence field. A technical arrangement on the sharing of non-classified information between NCIRC and the EU CERT has been in operation for over one year and the recent Action Plan to implement the NATO EU Joint Declaration, agreed by NATO and the EU in December 2016, provides for more NATO EU interaction — for instance, in sharing information on operational planning for cyber defence during military missions, harmonising 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 and Cyber Coalition and the EU's Cyber Europe.

WORKING AT THE TOP BUT ALSO AT THE BOTTOM

In conclusion, cyber is different from the other domains of conflict. The pace of innovation is much faster. The technology is much more decentralised and many more actors are involved, for better and for worse. Resources need to be spread over a far greater number of functions and applied much more selectively than in a conventional capability programme 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 hacking during the 2017 US 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 as an act of aggression and elicit an appropriate response. Whereas we have a good idea how to deter a nuclear attack or a conventional attack, or to deal with crises in the traditional domains, and we know what kind of arms control or confidence-building arrangements can be useful to keep things peaceful, we still do not have a good idea how we can 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 not to do it; we can impose sanctions against certain individuals or organisations, as the US has done in response to the Yahoo attack and the election interference; but if the gains are seen to significantly outweigh the risks, then deterrence is not going to work. 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 basic problems that we have been confronting for the last 20 years or so. In the first quarter

of 2016, there was a 250 per cent increase in the number of phishing sites and related e-mail traffic *vis-à-vis* the final quarter of 2015. The most recent McAfee labs threats report warns that for every ten phishing e-mails sent by attackers, at least one will be successful. McAfee presented ten real e-mails 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 per cent incorrectly identified at least one phishing e-mail. According to Verizon, 30 per cent of phishing messages are opened and around 12 per cent allow the attack to succeed by clicking the malicious attachment or link. In 2016, there was a 400 per cent spike in ransomware families, with 15 new ones discovered on average every month. Meanwhile, DDOS attacks are becoming larger and the average payout from business e-mail compromises is now running at US$140,000. 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, as with most other organisations, to work increasingly 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 US 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 e-mail was real or fake. So there is a lesson here for all of us that we will never have effective cyber defence 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. I began this paper by referring to years of decision and years 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 cyberthreat.

Acknowledgement

The views in this paper are entirely those of the author alone. They should not be construed as representing an official position of NATO but are contributed in a purely personal capacity.