THE TALLINN PAPERS
A NATO CCD COE Publication on Strategic Cyber Security

JAMES A. LEWIS

THE ROLE OF OFFENSIVE CYBER OPERATIONS IN NATO'S COLLECTIVE DEFENCE

Tallinn Paper No. 8
2015

CCDCOE
NATO Cooperative Cyber Defence
Centre of Excellence Tallinn, Estonia

Previously in This Series

No. 1 Kenneth Geers “Pandemonium: Nation States, National Security, and the Internet” (2014)

No. 2 Liis Vihul “The Liability of Software Manufacturers for Defective Products” (2014)

No. 3 Hannes Krause “NATO on Its Way Towards a Comfort Zone in Cyber Defence” (2014)

No. 4 Liina Areng “Lilliputian States in Digital Affairs and Cyber Security” (2014)

No. 5 Michael N. Schmitt and Liis Vihul “The Nature of International Law Cyber Norms” (2014)

No. 6 Jeffrey Carr “Responsible Attribution: A Prerequisite for Accountability” (2014)

No. 7 Michael N. Schmitt “The Law of Cyber Targeting” (2015)

Disclaimer

This publication is a product of the NATO Cooperative Cyber Defence Centre of Excellence (the Centre). The expressions reflected are those of the author(s) alone; publication by the Centre should not be interpreted as endorsement thereof by the Centre, its Sponsoring Nations or NATO. The Centre may not be held responsible for any loss or harm arising from the use of information contained in this publication and is not responsible for the content of the external sources, including external websites referenced in this publication.

Digital or hard copies of this publication may be produced for internal use within NATO and for personal or educational use when for non-profit and non-commercial purpose, provided that copies bear a full citation.

Please contact publications@ccdcoe.org with any further queries.

The Tallinn Papers

The NATO CCD COE's *Tallinn Papers* are designed to inform strategic dialogue regarding cyber security within the Alliance and beyond. They address cyber security from a multidisciplinary perspective by examining a wide range of issues, including cyber threat assessment, domestic and international legal dilemmas, governance matters, assignment of roles and responsibilities for the cyber domain, the militarisation of cyberspace, and technical. Focussing on the most pressing cyber security debates, the Tallinn Papers aim to support the creation of a legal and policy architecture that is responsive to the peculiar challenges of cyberspace. With their future-looking approach, they seek to raise awareness and to provoke the critical thinking that is required for well-informed decision-making on the political and strategic levels.

Submissions

The Tallinn Papers is a peer reviewed publication of the NATO Cooperative Cyber Defence Centre of Excellence. Although submissions are primarily commissioned by-invitation, proposals consistent with the annual theme and dealing with issues of strategic importance will be considered on an exceptional basis. Since the Tallinn Papers are meant for a wide audience, such proposals should assume no prior specialised knowledge on the part of the readership. Authors wishing to submit a proposal may contact the Editor-in-Chief at publications@ccdcoe.org.

The Role of Offensive Cyber Operations in NATO's Collective Defence

James A. Lewis[1]

New military technologies are destabilising. Computers used for attack are one such technology. NATO has made considerable progress in its efforts to integrate cybersecurity into its planning processes, but while it may have gone as far as the political environment allows, it needs to do more. NATO's September 2014 summit established that cyber defence is part of the Alliance's core tasks of collective defence, crisis management, and cooperative security. Consistent with its long history as a defensive organisation, the policy emphasised "prevention, detection, resilience, recovery."[2]

Cyber defence has become a central component of NATO planning, given the success of Russia and others in compromising NATO networks. US intelligence sources assess that any unclassified NATO network that is directly connected to the internet should be considered potentially compromised and that cyber espionage is the principle threat to NATO systems over the next three years. They also assess that Russia, given its record of effective cyber collection, poses the greatest espionage threat to NATO computer networks.[3] The vulnerable state of many NATO members' national networks makes defence a priority, but it cannot be the only priority. Discussion within NATO has focused on a defensive role and on the issue of when a cyber incident could trigger the collective defence provision of Article 5 of the North Atlantic Treaty. NATO's Computer Incident Response Capability (NCIRC), co-located with Allied Command Operations (ACO), is responsible for defending NATO networks. NATO is improving its cyber defence and helping member states improve their own cyber defences through information sharing, training, and if necessary, the deployment of rapid reaction cyber defence teams. These topics are essential for planning purposes, but leave NATO in a reactive mode when it comes to cyber

[1] Director and Senior Fellow, Strategic Technologies Program, Center for Strategic and International Studies.

[2] Wales Summit Declaration (5 September 2014), pt. 72, available at http://www.nato.int/cps/en/natohq/official_ texts_112964.htm.

[3] Private conversations with US officials.

warfare.[4]

The central question for NATO's cyber doctrine is how the lack of an articulated offensive cyber capability affects its ability to deter or defend. Put another way, can any military force credibly claim to have advanced capabilities if it does not include offensive cyber operations in its arsenal? Offensive capabilities, unlike NATO's current defensive posture, involve deliberate intrusions into opponent networks or systems with the intention of causing disruption, damage or destruction. The question of NATO and offensive cyber capabilities touches on a range of sensitive political issues that militate against any change in policy in the near term.

The US has always been overly secretive about its offensive cyber capabilities, even after a flood of media leaks have made the most sensitive doctrine publicly available. This secrecy has carried over into NATO, and is unhelpful in that it increases the likelihood of opponents miscalculating as they consider the risks of using force or coercion against NATO members or interests. A lack of public discourse on offensive cyber operations undercuts the legitimacy of NATO operations by failing to build public understanding, and leaves NATO open to charges of sinister plots, since denial of offensive capabilities is not credible when two NATO members are world leaders in cyber operations.

Parallels between cyber operations and nuclear strategy are usually misleading, but cannot always be dismissed. The parallel for NATO is that cyber attack is a "weapon" with both strategic and tactical uses, which only a few NATO members possess. Unlike nuclear weapons, however, the procedures for integrating offensive cyber operations into NATO's defensive actions are not at all obvious, if they exist. NATO will need to describe how the cyber capabilities possessed by a few of its members will support NATO's defensive activities, and NATO's credibility in defence requires some public discussion on the use of offensive cyber operations.

There has been a confusing debate over the merits of cyber deterrence, but one conclusion that we can draw from this discussion is that both the contribution of cyber operations to deterrence and the ability to deter cyber attack work best when embedded in a larger military force structure. Adding offensive cyber capabilities to NATO's force structure and response doctrine will increase its deterrent capabilities – by how much is unclear, but what is clear is that a failure

[4] Jason Healey and Klara Tothova Jordan, 'NATO's Cyber Capabilities: Yesterday, Today and Tomorrow,' Atlantic Council (September 2014), available at http://www.atlanticcouncil.org/images/publications/NATOs_Cyber_Capabilities.pdf.

to add cyber capabilities will erode a credible deterrent as cyber operations are increasingly embedded into military operations.[5]

Beyond deterrence, two other factors point to the need for additional consideration of NATO's public posture on offensive cyber operations. The first is that cyber techniques are essential for the kinds of combat operations that NATO forces may carry out in the future. No modern air force would enter into combat without electronic warfare (EW) capabilities; as cyber and EW merge into a single activity, air operations will require cyber support. The same is true for special forces operations. Offensive cyber capabilities will shape the battlefields of the future.

Second, NATO's potential opponents will use cyber techniques in new ways, in what some have called "hybrid warfare".[6] These include countries traditionally of concern to NATO, but cyber threats could also come from new actors, such as Iran or North Korea, and proxy or non-state actors such as the Syrian Electronic Army. These nations and groups, using cyber techniques, now have new ways to strike NATO countries.

Military doctrine is changing as opponents seek to circumvent US military power and use a blend of political action and "influence operations", special forces, proxies and irregular units, unconventional tactics and cyber techniques to apply force to gain their ends. Cyber techniques for political action and "influence operations" are not intended to destroy or disrupt, but rather to put coercive political pressure on targets. This new style of warfare will challenge planning for mutual defence. For these reasons, the need for more than defensive or technical cyber capabilities will increase.[7]

Offensive Cyber Operations

As militaries discovered the advantages of the information superiority (provided in good measure by computer networks) and built the network infrastructure to provide these advantages, they have also created a new "attack surface", which opponents can exploit. Cyber attacks will serve several purposes. Most cyber

[5] Henrik Ø. Breitenbauch, 'NATO: Conventional Deterrence is the New Black,' *War on the Rocks* (14 April 2014), available at http://warontherocks.com/2014/04/nato-conventional-deterrence-is-the-new-black.

[6] Michael Miklaucic, 'NATO Countering the Hybrid Threat' (23 September 2011), available at http://www.act.nato.int/nato-countering-the-hybrid-threat.

[7] NATO, 'Improving NATO's Capabilities' (16 February 2015), available at http://www.nato.int/cps/en/natohq/topics_49137.htm?selectedLocale=en.

attacks will not produce destructive effects similar to kinetic weapons, but will instead seek to disrupt data and services, sow confusion, damage networks and computers (including software and computers embedded in weapons systems) machinery. Offensive cyber operations would strike military, government and perhaps civilian targets such as critical infrastructure in the opponent homeland used to support war efforts.

"Tactical" operations would be undertaken to support combat forces and to shape the battlefield by degrading command networks and weapons software. Cyber actions at the tactical or operational level will be used against deployed forces and their support: the most likely form of attack will be against command and control systems (including sensors and computer networks) and against the software that runs advanced weapons such as surface-to-air missiles or fighter aircraft.

Strategic operations can be used in long-range[8] "strikes" against rear areas or the opponent's homeland, including against civilian targets. In this, cyber attacks could mimic strategic bombing, but the intention would be to disrupt services and degrade morale rather than cause mass destruction. US thinking about "strategic bombing" has evolved under the influence of precision guided munitions to focus on a narrower set of targets – "war-supporting infrastructure" – that could include electrical power grids and power generation facilities, telecommunications and financial systems, transportation systems and government networks. These civilian targets remain attractive objectives for cyber attack in support of military operations.

Opponent Use of Cyber Operations

Warsaw Pact doctrine during the Cold War contemplated the use of initial chemical weapons strikes against telecommunications and transport hubs and government centres as an opening move in any conflict. The doctrine of today's potential opponents includes plans to use cyber attacks to shape the initial phases of conflict and disrupt NATO's response. Strikes against civilian targets risk escalating any conflict, but an opponent may judge the risk of escalation to be acceptable if the context for cyber attack is an offensive against a smaller nation, such as a Baltic country, that it plans to rapidly overrun and occupy. Cyber strikes against civilian targets in these countries could provide a few hours

[8] The concept of "range" in cyber attack is complicated by the fact that fibre-optic communications travel, with some inefficiencies, at the speed of light. This means that any connected system or network anywhere on the planet is within "range".

or even a few days of disruption that would in turn generate real advantage in operations planned to last only a day or two. Cyber actions against NATO's supporting infrastructure, to slow the response to such an offensive, are also likely, but an opponent may choose to limit the effects of such actions in the hopes of reducing the risk of escalation.

While NATO's likely opponents include those who will make extensive use of cyber techniques, it is worth bearing in mind that the use of offensive cyber capabilities has been minimal in recent armed conflicts in Europe, and has been used primarily for political coercion, opinion shaping and intelligence gathering. Unless new opponents badly misinterpret NATO's resolve, a *blitzkrieg* against NATO states is unlikely; but the kind of hybrid warfare used against Ukraine remains a very real risk. Operations in Georgia and Crimea suggest that we need to adjust our thinking about an opponent's use of cyber attacks.

The doctrine of nations hostile to NATO also includes the use of offensive cyber activity for pre-conflict and "opinion-shaping" during the course of conflict, to shift public judgments in NATO countries as well as globally in ways favourable to the attacker, and to create a sense of unease and distrust among allies. These actions could be used in isolation without being linked to conventional military action, as in Estonia in 2007, or as an accompaniment to a conventional campaign, as in Georgia. Stories about the plight of oppressed minorities and the intransigence and hostility of the target government will appear in Western press outlets and on social media sites. Damaging emails obtained through cyber espionage will be leaked or fabricated when necessary.

The emphasis is on political action and opinion shaping, seeking to portray the other side as fascists and human rights violators against whom an oppressed population has risen in defiance. The US, NATO, and the West are characterised as interlopers, seeking only to extend their hegemony and weaken the sovereign rights of other nations. Such charges are intended to support the aggressor narrative and create dissension among Western nations. Western military forces and governments are ill-equipped to respond to this.[9]

Cyber operations used for coercive effect create uncertainty and concern within the target government. The knowledge that an attacker may have infiltrated their networks, is monitoring communications, and perhaps considering even more damaging actions, can have a paralysing effect. The vast majority of these cyber operations are likely to fall below the level of an armed attack, even

[9] Peter Pomerantsev, 'Yes, Russia Matters: Putin's Guerrilla Strategy,' *World Affairs* (September/ October 2014).

under the new NATO guidelines, complicating any response. The effort to gain information superiority falls in good measure outside of NATO's purview, but the Alliance must take these into account in planning for the role of cyber activities in conflict.[10]

Stabilising or Not

Dissimulation is an essential part of hybrid warfare, and Europe and the US face a propaganda barrage that is much more sophisticated than the clumsy Soviet efforts of the Cold War. Despite this clumsiness, a good portion of the Western public has found it persuasive. Similarly, those critical of NATO will find new complaints about aggression and militarisation credible. Russia has already complained that NATO's defensive cyber doctrine is destabilising war-mongering and part of a larger conspiracy to advance western hegemony.[11] The Snowden revelations have lent a powerful impetus to Russian propaganda.

Behind the rhetoric lies both a desire to conceal their own use of cyber operations and a real fear that Russia's decline leaves it vulnerable to new military technologies. The intent is to hamper and complicate any Western response to Russian efforts to regain control in Crimea and the "near abroad". The Russian position is that NATO's new cyber doctrine is destabilising as it threatens to use conventional or even nuclear responses (in the Russian description of the new policy towards low-level cyber attacks).

Any announcement by NATO relating to offensive cyber capabilities would be greeted with alarm and vitriol in Moscow. However, the effect on stability would likely be less pronounced. NATO-Russia relations are already in steep decline. It is possible that any NATO announcement would accelerate this, but it is also possible that Russia could recalculate the risk of further adventures if it were faced with a stronger defence. In terms of opponent attitudes, there is probably little effect. Russia, along with NATO's other potential military opponents, is likely to overestimate both capabilities and coordination among NATO member states and underestimate NATO's will to defend. This is an unhappy

[10] See, *e.g.*, Hannes Krause, 'NATO on Its Way towards a Comfort Zone in Cyber Defence,' Tallinn Paper No. 3 (2014), available at https://ccdcoe.org/multimedia/nato-its-way-towards-comfort-zone-cyber-defence.html; NATO, *supra* note 3; Steve Ranger, 'Exploit a flaw or go to war? NATO's cyber battle rules raise more questions than they answer,' *ZDNet* (2 September 2014); Leo Cendrowicz, 'NATO frontline in life-or-death war on cyber-terrorists,' *Guardian* (30 October 2014); Josephine Wolff, 'NATO's Empty Cybersecurity Gesture,' *Slate* (10 September 2014).

[11] Private discussions with senior Russian diplomats.

combination as it makes aggression against NATO seem less risky.

NATO's decision on how cyber attacks could trigger Article 5, while greeted with complaints, had a stabilising effect. It made clear to potential opponents that cyber attacks are not risk-free. Similarly, a clear enunciation of how NATO would use offensive cyber capabilities as part of any defensive operation would also change opponents' risk calculations in ways that would force them to consider how offensive actions, even if intended to be covert, are not free of risk or cost.

The Cyber Club

Some level of cyber capability is being acquired by all advanced militaries, and perhaps a dozen countries can be identified from public sources as procuring offensive cyber capabilities. These countries include several NATO members. As with nuclear weapons, the capability to undertake offensive cyber operations is a club within a club in NATO, with largely the same membership – the US, the UK and France. Germany's armed forces may also be developing offensive cyber capabilities.[12] The well-developed procedures for release and for integration into NATO planning created for nuclear weapons do not exist for cyber attack, although it is currently far more likely that any NATO military operation will have a cyber component, while the use of nuclear weapons is almost unthinkable.

The US and the UK both possess elite cyber capabilities. They also have a close partnership in cyber espionage. This partnership is centred on a relationship between the US National Security Agency (NSA) and the British Government Communications Headquarters (GCHQ), both of which are intelligence agencies with a long history of supporting military operations. US military cyber operations are the responsibility of U.S. Cyber Command, whose commander is also the head of the NSA. Cyber operations blur the line between intelligence and military activities. The fact, however, that these are intelligence agencies has a created a certain reticence regarding the sharing of information on capabilities and plans, which complicates the integration of offensive cyber into NATO planning and doctrine.

Offensive cyber capabilities are still too new, with too many unknown risks that hold potentially profound political consequences. US policy is that only the President can approve a cyber operation likely to result in "significant

[12] John Goetz, Marcel Rosenbach and Alexander Szandar, 'War of the future: national defence in cyberspace,' *Spiegel Online* (11 February 2009).

consequences" that could produce loss of life or a damaging reaction, although the Secretary of Defense or the head of U.S. Cyber Command can take independent action in an emergency. US policy restricts independent action by tactical and operational commanders for this reason. A local commander may not know all the trade-offs or the risks that using a cyber attack could entail. That said, all of these problems are manageable with some decision-making model based on the precedent of the warning and request system used for nuclear weapons release.[13]

Until there are better predictive tools and judgments about risk and consequences, offensive cyber operations will require a politically sensitive decision as to when the benefit of an attack outweighs the political risk. Additional coordination mechanisms would be needed to decide when the benefits of an attack outweigh the risk of a loss of intelligence capabilities, or when a target justifies expending a weapon that might never work again. The inability to predict collateral damage and uncertainty over political effect encourage caution in the use of offensive cyber operations, but that is not the same as advertising possession of the capability.

Whiskey and Romeo

It could be argued, given NATO's defensive orientation (*pace* Russian fears of diabolic plots), that a purely defensive and technical focus for cyber operations is appropriate. The question, however, is whether NATO can field a credible military force without some public linkage to an offensive cyber capability.

Here again, the nuclear precedent offers some suggestions for a way forward. In the NATO phonetic alphabet, "whiskey" ("W") and "romeo" ("R") were used by NATO's command structure in conflict to "warn" capitals that with a deteriorating situation on the ground it would be sending a request to release nuclear weapons for NATO use. Romeo was the actual request for release of nuclear weapons to NATO control. This terminology prepared nuclear capitals to make the decision on release.

Just as nuclear weapons remain under national control but senior NATO commanders can request their release, the US and UK could retain control of offensive cyber capabilities but be prepared to make them available to NATO commanders upon request. In practice, national teams could be assigned to support NATO commanders in theatre or could carry out some operations against targets selected by NATO commanders form their national duty station.

[13] Department of Defense, 'Cyberspace Operations' (February 2013), Joint Publication 3-12(R), available at www.dtic.mil/doctrine/new_pubs/jp3_12R.pdf.

Such an arrangement needs more than *ad hoc* coordination. It requires an identified structure for request and release that is regularly practised. It demands offensive cyber operations used for defence purposes to be included in planning and exercises. It would also be beneficial for NATO's defence mission if the exercise of systems for the use of offensive cyber capabilities in support of defensive operations was made public.

Cyber operations necessitate advance planning and practice, particularly for multinational operations that are already inherently complex in their coordination and de-confliction requirements. Offensive cyber operations create conflicts between goals and missions for the use of cyber techniques. The fundamental decision is whether to collect intelligence or to engage in military operations. This creates an immediate problem for NATO, because decisions on intelligence collection will be taken at the national level whereas military operations are in the purview of the NATO military command structure. This consideration would necessarily be part of the decision process in national capitals, which would likely be an iterative process to allow for additional input from the theatre of operations.

The similarity of cyber operations with nuclear weapons lies not in destructive power – a cyber attack would not cause anywhere near the damage that even a small nuclear warhead would produce – but in the need for political control of release and use. The effects of a cyber attack, while limited, are still somewhat unpredictable. The risk of collateral damage is difficult to estimate. Computer networks are connected in strange ways and therefore we could attack one network only to find that third party networks depend on it. This uncertainty about effect is a constraint on offensive cyber operations.

The nuclear precedent involves the onset of conflict and a warning from a senior NATO commander to nuclear capitals that they might need to use nuclear weapons. This would be followed by a request for the use of nuclear weapons for use in combat. While the entire process would be relatively speedy, taking only a few hours, this might be too long for some cyber operations. The dilemma with cyber operations is that, unlike in the case of nuclear weapons, where the time between warning, request, release and use could be measured in hours, preparation for and deployment of a major cyber attack may take weeks or months. Cyber attacks have several stages: reconnaissance to identify the target's vulnerabilities, developing "weaponized" code, breaking in, delivering the software "payload", and then "triggering" it – all without being detected. The most harmful cyber attacks – those like Stuxnet that cause physical damage – are still a high art of which only a few nations are capable. While it may eventually be possible to refine the ability to quickly deliver cyber effects and to better estimate the potential for collateral damage, the requirements for preparation limit the utility of the nuclear release model for advanced cyber attacks and highlight the need for advance coordination and planning.

Beyond the Nuclear Precedent

A better approach would be for the nations with cyber capabilities to dispatch teams to support the NATO commander, operating under general instructions on what kinds of operations and target are permissible in support of NATO military activities but delegating specific support action to the purview of the NATO commander. This follows the precedent developed in the US for Cyber Command providing cyber capabilities to regional combatant commanders.

It is possible that such arrangements already exist on a classified basis. That said, there might be an advantage for NATO's deterrent capabilities from making public some general description of these arrangements. NATO could also benefit from ensuring that its exercises include an offensive cyber component. This does not mean, despite Russian suspicions, that NATO will plan offensive cyber operations. It means that just as NATO aircraft are not confined to a defensive tactical role in responding to an attack, a "counter-offensive" capability will require a cyber component. NATO will not initiate conflict, but if conflict is initiated by an opponent, NATO defences will be best served by including an offensive cyber component in its planning and operations.

Public acknowledgment by NATO of a new role for offensive cyber capabilities in collective defence is a politically sensitive question. It took, after all, more than six years for NATO to decide on the issues on Article 5 raised by the Estonian incident. Since 2007, the technology for cyber attack, the number of countries which can use it, and the political-military situation in Europe have changed dramatically. NATO may still have the luxury of a lengthy debate over offensive capabilities – it likely has no other choice – but the risk created by delays in building adequate defences during long deliberation is greater than it was in 2007.

One possible explanation for this is that there is neither expectation nor intent for NATO to engage in major military operations, and therefore no need to plan for the use of cyber attack. The parlous state of the forces of many NATO members could open questions about NATO's conventional deterrent capabilities, even with the addition of offensive cyber capabilities.

A NATO Cyber Red Team created to test defences would provide an incipient offensive capability, but this by itself is not enough. A Cyber Red Team allows individuals and teams with both the capability to break into networks and the opportunity to practise their techniques, but it does not embed them in a planning and operational context, nor does it connect them to the intelligence needed for a successful cyber attack. It could be difficult to quickly transform a Red Team into an offensive military capability embedded in the operational planning process, especially if this had not been practised in advance. Even if we assume that NATO has an unpublicised offensive capability, there would still be benefit to be gained from both open discussion and declared policy.[14]

It may be politically astute for NATO to hold to a tacit renunciation of offensive cyber operations, something non-governmental organisations and advocates of notions like "non-offensive defence" would like to see. Cyber arms control is unlikely, however. Verification remains almost impossible. The use of proxies provides a degree of political complication, as Western public opinion may demand an unrealistic level of evidence, and this could encourage opponents to attempt to evade any commitment to limit the use of cyber weapons.

The most we can expect is agreement on confidence-building measures (CBMs) and on the application of international law to cyber operations. While there was good progress in the Organisation on Security and Cooperation in Europe in agreeing on an initial set of CBMs, events in Crimea have derailed the cooperation needed for further progress. Renunciation of cyber attacks will not change this and unilateral restraint will not be reciprocated.

Any conflict among advanced military powers will include cyber activities. Reticence about discussing offensive cyber operations may also reflect the nature of cyber attacks, where cyber capabilities can be closely linked to highly classified national intelligence activities, making those few nations that possess them reluctant to share. Most advanced "cyber powers" programmes blend warfighting and covert action in their cyber war planning. The close connection to espionage works against discussion of offensive capabilities and their incorporation into NATO planning.

NATO developed complex but efficient mechanisms to allow the tactical use of nuclear weapons. Cyber attacks are not like nuclear weapons, and with more experience and a better ability to predict, there might be circumstances in which the US or UK could consider allowing NATO commanders to use offensive cyber capabilities. This will require answers to a number of significant questions

[14] See, *e.g.*, NATO, 'NATO Rapid Reaction Team to fight cyber attack' (March 2012), available at http://www.nato.int/cps/en/natolive/news_85161.htm; NATO, 'North Atlantic Council visits NATO cyber security centre' (January 2015), available at http://www.nato.int/cps/en/natohq/news_116790.htm?selectedLocale=en.

on the risk of damage to unintended targets, conflicting missions and goals, and the actual requirements and costs of the cyber attack itself.

Building a Responsive Cyber Defence

The nature of warfare is changing as opponents seek to circumvent Western military power by using a blend of political action, special forces, proxies and irregular units, unconventional tactics and cyber techniques to find a different way of applying force to gain their ends. What Russia sometimes call "hybrid warfare" will challenge NATO defence planning. A cyber defensive orientation is, however, the equivalent of a static defence, defending fixed positions rather than manoeuvring, and conceding initiative to opponents. The next public iteration of NATO cyber policy should describe how NATO members with offensive cyber capabilities would retain national control, but make these capabilities available to NATO in the event of aggression. NATO should be more explicit in how offensive cyber operations fit into its defensive and deterrent strategy. Finally, it needs to identify and describe a regular coordinating process to be established (similar to the Nuclear Planning Group) in NATO's Cyber Defence Committee (CDC).

NATO would never refrain from using fighter aircraft because they can serve offensive purposes, and say it would rely solely on air defence missiles and damage control to deal with the threat of air attack. Nor would NATO renounce armoured vehicles and rely only on static defence. A defensive approach that forsakes the possibility of offensive action is essentially a cyber Maginot Line. This defensive orientation serves no one's interest except that of our opponents. Offensive cyber operations are similarly a part of warfare that advanced militaries cannot ignore. The mechanisms for incorporating offensive cyber into NATO will be complicated by national sensitivities, and public presentation will need to be carefully crafted to reinforce a deterrent message; but the next step, however politically difficult, for NATO transformation is to publicly embrace offensive cyber capabilities in planning and exercises.

Warfare is evolving as technological and political developments change the requirements for effective operations. Military innovations create a new dynamic for calculating risk among potential adversaries. Forces and concepts that once seemed adequate for stability are called into question. It will be neither easy nor quick for NATO to discuss publicly the role of offensive cyber operations, but it is ultimately unavoidable.