PISM POLSKI INSTYTUT SPRAW MIĘDZYNARODOWYCH
THE POLISH INSTITUTE OF INTERNATIONAL AFFAIRS

BULLETIN

No. 71 (803), 10 July 2015 © PISM

NATO Policy on Cyberattacks: Defence and Deterrence

Artur Kacprzyk

Amid growing threats online, NATO made a ground-breaking declaration at the Wales summit, allowing the invocation of Article 5 in the event of the most serious cyberattacks. In the context of next year's Warsaw summit, the implementation of the Enhanced Cyber Defence Policy requires not only a determination of the forms of collective response to different kinds of cyberattacks, but also strengthening of the Allies' defence capabilities and further development of NATO's assistance instruments.

The Threats. Online attacks are becoming increasingly numerous and advanced. Most intrusions into NATO systems, and into the government networks of its members, are acts of espionage, aimed at obtaining classified data, such as the theft of the personal data of around 4 million U.S. federal workers from the database of the Office of Personnel Management (OPM), discovered last April. In the same month, the airline Ryanair confirmed the theft of $5 million from its bank account, which is an example of activities carried out by financially motivated cybercrime groups, regularly targeting the private sector and individuals. There are also numerous acts of online vandalism (such as denial of access to websites, defacement, or data destruction), perpetrated by individual hackers and groups sympathising or cooperating with states or terrorist organisations. For example, in January, hackers posted pro-Islamic State propaganda on social media accounts of U.S. Central Command (CENTCOM), responsible for military operations in the Middle East.

In the future, however, destructive cyberattacks could be used to destabilise of intimidate NATO countries in peace time, or to support military actions against the Alliance. Such capabilities are being developed by NATO's potential adversaries, such as Russia and Iran, while conflicts in Georgia (2008) and Ukraine (2014-2015) prove the on-going integration of cyber and conventional operations. The main targets of possibly the most severe attacks include military networks and systems of civilian critical infrastructure. Deletion and manipulation of data, or seizure of control of networks, could paralyse command and communication systems, or deprive societies of access to energy, financial and communication services.

Although there have so far been no reports of cyberattacks leading to major disruption of critical sectors or losses of life and widespread physical damage, capabilities to undertake such attacks are becoming increasingly advanced. Examples include reports on an Israeli cyberattack that disabled Syrian air defences before an airstrike on Al Kibar nuclear reactor in 2007, as well as an attack that exposed flaws in Saudi Arabia's critical infrastructure systems by deleting data from 30,000 of oil company Aramco's computers. The existence of a "cyberweapon" has been primarily shown by the Stuxnet worm, which reportedly destroyed around 1,000 uranium enrichment centrifuges at the Iranian Natanz facility.

Difficult Beginnings for NATO's Cyberdefences. NATO's main task is to protect its own networks and to assist its members in the development of their national cyberdefence capabilities, intended to secure networks, detect attacks, ensure continued operation in the event of an attack, and recover attacked systems. NATO's support includes, among other things, facilitating the sharing of information and best practices, setting common protection standards for national networks critical for NATO missions, and organising cyberdefence exercises. With respect to the protection of its own networks, the Alliance was acting even before adopting its first cyberdefence policy in 2008, by establishing a NATO Computer Incident Response Capability (NCIRC) in 2002, which achieved its full operational capability in 2014. In 2012,

one year after updating the cyberdefence policy, NATO set up two six-man rapid reaction teams (RRTs), which can be deployed on the North Atlantic Council's approval to assist members suffering from significant attacks.

Under the Enhanced Cyber Defence Policy, adopted at the Wales summit in September 2014, the responsibility for protection of national networks still rests with the Allies themselves, although they can count on greater assistance from NATO than before. Such support is necessary, since many states, especially the smaller ones, have not developed adequate capabilities due to cuts in defence budgets and lack of expert capacity. Moreover, the unwillingness of the biggest Allies to share sensitive information (on threats and their own capabilities) impedes preparations for cooperation in a crisis, including the complex integration of cyberdefence into planning of territorial defence and crisis management operations.

Hence, the new policy emphasises intensified exercises with the use of an Estonian cyberdefence training ground, aimed at building trust and interoperability among the Allies. NATO also aims to enhance educational and consultancy support, provided by, among others, the NATO Cooperative Cyber Defence Centre of Excellence (CCD COE) in Tallinn. The Alliance also sets development targets for national cyberdefence capabilities, within the NATO defence planning process (NDPP). Additionally, a promising signal is that three groups of Allies have started collaboration on common capabilities, within the framework of Smart Defence initiative projects. These capabilities include a Malware Information Sharing Platform (MISP), Multinational Cyber Defence Capability Development (MN CD2), and Multinational Cyber Defence Education and Training (MN CD E&T).

NATO's new priorities also cover enhanced cooperation with international partners, including the EU, which is developing its own cybersecurity policy. An area of key importance is more intense cooperation with industry, within the NATO Industry Cyber Partnership (NICP), launched in September 2014. Its implementation is important in the light of the development of new cyberdefence capabilities for NATO, but also given that most of the critical infrastructure is operated by private companies. Therefore, it is crucial for both sides to prepare for cooperation in the event of cyberattacks (such as, by sharing information on threats).

Deterrence Problems. Cyberdefences being developed by the Alliance are potentially also an instrument of deterrence by denial, as they could convince an adversary that an attack would be ineffective. However, many Allies lack effective defences, and a potential aggressor could still decide to attack, as failure would not result in serious consequences for the attacker. By declaring that a cyberattack can trigger NATO's collective response, the Alliance strengthens the other form of deterrence, that is deterrence by punishment, intended to convince the enemy that even a successful attack would result in severe retaliation.

Nonetheless, the Wales summit declaration does not define, specifically, how damaging a cyberattack must be to trigger the invocation of Article 5 and it notes that a decision on collective response would be taken by the North Atlantic Council on a case by case basis. It also emphasises that the impact of cyberattacks could be comparable to the effects of conventional attacks. Such a formulation only suggests that NATO could react in the event of an attack resulting in human casualties and physical damage, leaving even greater doubts about the possibility of a response to attacks with major consequences on networks or other digital infrastructure (such as paralysis of a banking system).

The ambiguity of cyberdeterrence is, however, a logical move by NATO, as it aims to keep the adversaries guessing about whether NATO would respond to their actions. Adoption of a certain threshold triggering retaliation could signal to the perpetrators of less severe attacks that they will remain unpunished. Moreover, a response requires attribution of the attack to a particular adversary, which will try to hide its involvement. In some cases, the source of the attack could be clear, especially given that only states possess human and material resources necessary to carry out the most destructive strikes, which would most likely occur during significant political tensions. Still, in some situations, NATO Allies might be uncertain about whether an attack had been launched by a specific state or, for example, by hackers supporting that country.

In consequence, the Allies should not change the provisions of the deterrence policy, but rather they conceptualise a specific cyberdefence doctrine, by agreeing, within the Alliance, which attacks would prompt NATO's response and what form it would take. The states will most likely not be willing to use conventional forces, if the cyberattack doesn't cause widespread physical damage and human casualties. A potential response to a less severe, but still significant attack could be the use of cyberoffense capabilities. Such operations would be aimed at breaking into an aggressor's network in order to disrupt or degrade systems responsible for the initial attacks or other digital assets. It is not possible to create a NATO joint cyberoffense forces, as there is controversy regarding their legality (for example, they could be used in covert military operations, and the effects of their use could spread uncontrollably, causing disproportionate harm), and countries will be unwilling to share secret and costly cyberoffense technologies. Nonetheless, numerous NATO states possess and develop such means, especially the United States, which officially outlines such operations in its cyberstrategy. Hence, NATO should begin a dialogue on possibilities and mechanisms of the use of cyberoffense forces by individual countries as a part of collective defence. Still, the development of defensive capabilities should remain NATO's priority. Deterrence will not stop many smaller-scale attacks, such as acts of vandalism, crime, and espionage, or major strikes during open military conflict.