STC

064 STC 14 E
Original: English

NATO Parliamentary Assembly

SCIENCE AND TECHNOLOGY COMMITTEE

CYBER SPACE AND EURO-ATLANTIC SECURITY

DRAFT SPECIAL REPORT*

Philippe VITEL (France)
Special Rapporteur

www.nato-pa.int

30 April 2014

* Until this document has been approved by the Science and Technology Committee, it represents only the views of the Special Rapporteur.

TABLE OF CONTENTS

I. INTRODUCTION 1

II. CYBER SPACE AND NATIONAL SECURITY 1
A. THE GENERAL CYBER THREAT ENVIRONMENT 1
B. THE CYBER THREAT TO NATIONAL SECURITY 2
C. COUNTERMEASURES AGAINST CYBER THREATS TO NATIONAL SECURITY 3
1. Cyber Defence 3
2. Cyber Deterrence 4
3. Cyber Arms Control 6
D. THE PROSPECT OF INTERSTATE CYBER WAR 6

III. EURO-ATLANTIC DEFENSIVE RESPONSES 7
A. THE UNITED STATES 7
B. FRANCE 9
C. NATO 10
D. THE EUROPEAN UNION 11

IV. CONCLUSION 12

BIBLIOGRAPHY 14

I. INTRODUCTION

1. Over the last quarter-century, cyber space has become a fundamental pillar of modern life. It has turned into an integral part of the world economy, revitalised civil society in the industrialised world, spawned revolutions in developing countries, and opened new possibilities for governments to provide services to their citizens. In parallel to these positive developments, however, the threats to and in cyber space as well as the threats which are enabled by it have multiplied greatly. Undoubtedly, cyber-crime and espionage are the most pervasive cyber threats in existence today. It is estimated that "the cost of cybercrime and cyber espionage to the global economy is probably measured in the hundreds of billions of dollars" (CSIS/McAfee, 2013). Political cyber subversion is another growing phenomenon in the cyber world. The internet has made it possible to easily mobilise followers and to peacefully undermine the trust in a political system – whether the political cause is deemed 'legitimate' or 'illegitimate' naturally depends on one's perspective.

2. Acts of cyber-crime, industrial espionage, or subversion only rarely amount to threats to national security. Most of the time, such acts are a matter for law enforcement agencies. In contrast, the aim of this report is to examine those cyber threats that can directly undermine national security. Such cyber threats are continuously growing, and governments and international organisations around the world are wrestling with the question of how to counter them. More specifically, the report first examines the general cyber threat environment; the specific threats to armed forces and critical infrastructure, which are those threats that aim directly at a state's security; the possible countermeasures; and the prospect for interstate cyber war. Then, the report turns to the efforts undertaken by two NATO member states – the United States and France –, NATO itself as well as the European Union (EU), in order to illustrate how important international actors are dealing with the cyber threat.

3. This Special Report was prepared for the Science and Technology Committee (STC) of the NATO Parliamentary Assembly with the purpose of informing a transatlantic debate on the nature of the cyber threat and the ways in which co-ordinated and collective cyber security can enhance the security of the Euro-Atlantic area. Moreover, with this report your Rapporteur wishes to contribute to an informed and realistic public debate on cyber security. This report follows on from previous Assembly reports on cyber security – the 2009 Defence and Security Committee report on *NATO and Cyber Defence* and the 2011 Committee on Civil Dimension of Security report on *Information and National Security* –, the 2011 Assembly resolution on cyber security, as well as continuous coverage of this issue during Assembly meetings and missions.

II. CYBER SPACE AND NATIONAL SECURITY

4. To understand how states and international organisations can tackle cyber threats to national security, it is important to comprehend the general cyber threat environment, including how malicious computer code works; to examine the specific cyber challenges for the armed forces and critical infrastructure; and to conceptualise possible countermeasures. This section concludes with an analysis of whether full-fledged cyber war is a realistic possibility.

A. THE GENERAL CYBER THREAT ENVIRONMENT

5. Cyber space can be defined as "a global domain within the information environment whose distinctive and unique character is framed by the use of electronics and the electromagnetic spectrum to create, store, modify, exchange, and exploit information via interdependent and interconnected networks using information-communication technologies" (Kuehl, 2009). No one *unified* cyber space exists: the internet is the most pervasive cyber space, but not all networks are connected to it. On the contrary, the most critical networks are (or should be) isolated from the internet. Still, cyber threats to such networks are rising, as potentially hostile actors find new ways of gaining access.

6. Cyber threats against military networks and critical infrastructure span a range of acts, from cyber espionage and sabotage to acts that could be classed as a use of force or, *in extremis*, as acts of war. No known cyber-attack has yet been classified as a use of force or an act of war. Today, the overwhelming majority of security breaches has no direct physical impact and involves either espionage or the disruption of communication or other network services. Within this range of threats, it is important to carefully distinguish between two categories of hostile cyber actions, even if it is often difficult in practice. A cyber-attack "refers to the use of deliberate activities to alter, disrupt, deceive, degrade, or destroy computer systems or networks used by an adversary or the information or programs resident in or transiting these systems or networks" (Lin, 2012). To perpetrate a cyber-attack, malicious code is employed to threaten or cause "physical, functional, or mental harm to structures, systems, or living beings" (Rid, 2013). In contrast, cyber exploitation – or simply cyber espionage – "refers to deliberate activities taken to penetrate computer systems or networks used by an adversary in order to obtain information resident on or transiting through these systems or networks" (Lin, 2012).

7. To be successful, malicious computer code requires three components: a vulnerability, access, and a payload (Lin, 2010). By definition, malicious code does not work without a vulnerability – a defect or bug – in a targeted system. Herein lies a key difference between cyber and conventional threats. Saboteurs, spies, or non-cyber weapons do not need to take advantage of a fatal flaw to be successful, but if a computer network does not contain any flaw, it is immune to cyber-attack. That said, given the complexity of today's systems, it is highly unlikely, if not impossible, that computer networks do not contain any vulnerabilities which hostile actors could abuse. However, there is one exception: a denial of service attack, aiming to render a computer network unavailable, works by overwhelming the target with network traffic rather than by exploiting a vulnerability. Next, a hostile actor needs to gain access to the vulnerable system. Access can be gained remotely, for example through the system's connection to the internet or other open networks. Moreover, a hostile actor can also gain close access: an 'insider' could penetrate the system directly, by introducing malicious code to a system using a USB stick for example, or an external hostile actor could tamper with software or hardware components which later end up in the targeted system or become linked with it. Third, the hostile actor needs to insert a 'payload' which performs the desired malicious action. This could be installing surveillance software or breaking the system and perhaps injuring people as an indirect effect.

8. What makes cyber threats particularly unique is that they can originate from a wide variety of actors at all levels. Cyber-attacks are not the purview of states alone. Instead, low barriers to entry exist for potentially hostile actors. Malicious code is widely available, both openly and on a thriving black market. Even if such code is not freely available, an able hacker with few resources can easily develop his own code. Actors perpetrating cyber exploitation and attacks against armed forces or critical networks can include individual hackers, 'hacktivists', industrial spies, organised crime groups, terrorist organisations, national governments, and international organisations. This large variety of potential adversaries naturally poses unique challenges for governments. However, while all of these actors have the potential capability to stage cyber-attacks that could cause significant damage, offensive cyber programmes sponsored by governments remain the greatest worry, given the large resources a state can muster compared to non-state actors.

B. THE CYBER THREAT TO NATIONAL SECURITY

9. In general, a cyber threat to national security can arise if either military networks or critical infrastructure are targeted. Most other cyber threats can (and should) be handled by law enforcement agencies. Both the systems of the armed forces and critical infrastructure have specific characteristics that make them increasingly vulnerable.

10. In the armed forces, the importance of (and reliance on) cyber space is rising rapidly. Networked systems, devices, and platforms are already invaluable assets. However, the more the armed forces rely on networked capabilities, the more vulnerable they will become to potentially

devastating attacks. Indeed, the frequency of cyber intrusions in the military has risen dramatically, and the worldwide development of offensive cyber capabilities is progressing steadily. As any computer network, military systems are vulnerable to attack through the networks themselves and through software and hardware components, which could have been tampered with before they linked up with military systems. This threat is compounded by the fact that private entities own and operate the majority of communications and information infrastructure, and many components are obtained via global supply chains. Furthermore, while the most sensitive systems are in theory isolated from more open systems, they are nevertheless porous and a determined actor could find sufficient points of entry. Key challenges in this regard are therefore to keep hostile actors away from sensitive networks and increasing confidence that components have not been compromised.

11. Critical infrastructure, whether in private hands or government owned, is probably more vulnerable to cyber exploitation and attacks than the armed forces. While there is no common definition of critical infrastructure, the term generally covers those facilities and services that are vital to the basic operations of a given society or those facilities without which the functioning of a given society would be greatly impaired. Sectors that are often identified as essential include, but are not limited to, the sectors of government, energy, transportation, financial services, food, information, and communications. The cyber threat against these sectors is intensifying because of their increasing utilisation of information technology to manage and deliver services, adding to the attack surface of critical infrastructure and increasing the potential for cascading failures. Critical infrastructure is particularly vulnerable because owners, operators, and subcontractors increasingly use open source software or hardware, such as mobile phones or tablets, as well as and public networks in combination with or in lieu of private networks. This is of particular concern with respect to industrial control systems, for example so-called Supervisory Control and Data Acquisition (SCADA) systems. These systems are traditionally separate isolated networks. However, as more open networks promise numerous new possibilities, such as greatly improving efficiency, these systems are increasingly interconnected with other networks. All of these developments add to the vulnerability of critical infrastructure and increase the potential impact of a successful cyber-attack.

12. A key challenge in implementing a successful cybersecurity strategy for critical infrastructure is to find an effective way to manage the public-private relationship between the government on one side and the owners and operators of critical infrastructure on the other. Incentive structures differ in important ways between the two sides: governments are mostly concerned with security, but private companies need to watch their economic bottom line. Incentive structures differ in important ways between the two sides: governments are mostly concerned with security while private companies need to watch their economic bottom line. National governments and international organisations have the option of establishing either voluntary standards for cybersecurity, legislating mandatory regulations, or pursuing a hybrid policy combining the two former options. Given the rate at which information technology evolves and progresses, none of these options is an easy task.

C. COUNTERMEASURES AGAINST CYBER THREATS TO NATIONAL SECURITY

13. States have a number of ways to counter cyber threats to national security. Specifically, states can pursue cyber defence, cyber deterrence, as well as cyber arms control.

1. Cyber Defence

14. The first bulwark against cyber threats is a cyber defence which prevents hostile actors from succeeding in or at least from benefitting from their cyber intrusions. Governments and private defenders can take preventive and passive measures. States can improve their situational awareness of the cyber threat and invest into research and development of technologies that improve cyber defences. Organisations can create incentive structures that induce operators and customers to behave in conformity with basic cyber security requirements (Lin, 2012). For

example, the workforce can be trained in cyber 'hygiene'; audits can be performed to control and assess behaviour; and rewards can be handed out to increase compliance. On a technical level, cyber defences focus on remedying system vulnerabilities, for example by patching flawed software; closing off access routes, with firewalls for example; and thwarting payloads even if penetration was successful, for example by encrypting sensitive files or otherwise rendering them useless. So-called 'honey pots, which are decoys that lead intruders away from truly valuable information, can be planted, and software that can detect and survey intrusion can also be installed. To prevent cyber-attacks from causing unacceptable damage, states can also improve system continuity by increasing redundancy and resilience as well as their ability to repair and recover compromised systems.

15. Active cyber defence has drawn intensified attention. Aforementioned preventive and passive cyber defences are fundamentally reactive: organisations try to reduce vulnerabilities, block access points as well as minimise the lethality of payloads. However, determined cyber intruders are likely much more agile than cyber defenders and can rapidly adapt in order to circumvent new cyber defences. With active cyber defences, defenders could discover, define, analyse, and mitigate cyber threats in real time. Organisations could, for example, engage in 'hot pursuits' of an intruder, i.e. 'hacking back' into his own network, either openly or secretly. However, while active defences would enjoy a lot of advantages, the practical and legal ramifications are still unclear, especially for state actors (Farwell and Rohozinski, 2012). Under what circumstances would 'hacking back' constitute unwarranted cyber aggression? Who would have the authority to conduct active defence and under what circumstances? Where is the line between an active defence and a pre-emptive strike? These are some of the still questions that remain unresolved.

2. Cyber Deterrence

16. Many experts and government officials believe that the offense currently has the advantage in cyber space and that this is unlikely to change soon. As a consequence, cyber defences by themselves would be insufficient to keep would-be intruders out of critical infrastructure and military networks. Determined, proficient, and resourceful hostile actors would always find a way through cyber defences. This view is often combined with a belief that cyber-attacks can wreak extreme havoc at a moment's notice. Many experts and indeed governments therefore turn towards strategies of deterrence by punishment – in other words, strategies that attempt to prevent actors from conducting hostile cyber actions by threatening serious harm in return. Such retaliatory actions do not need to be restricted to actions in cyber space, but offensive cyber capabilities would certainly play a part in such a deterrence strategy.

17. Before laying out what a cyber deterrence strategy might look like and what challenges it would face, it is important to note that a growing number of analysts do not see the advantage of the cyber offence in such stark terms and caution against relying too heavily on cyber deterrence. They argue that the best defence is still a good defence. Sophisticated and thus more dangerous cyber weapons require a great deal of expertise to develop, and they would need to be tailored to very specific targets. Furthermore, the damage they can inflict is often uncertain, unpredictable, and often even counterproductive. Therefore, they would likely only inflict limited and highly targeted damage. The more sophisticated cyber weapons are the more opportunities to stop an attacker exist. As a consequence, these analysts argue, overreliance on cyber deterrence could lead to a sense of false security and could even have destabilising effects in a potentially adversarial relationship.

18. Despite these words of caution, many states seem to be developing or implementing cyber deterrence strategies. It therefore is imperative to understand the complexities and implications of cyber deterrence. In many ways, cyber deterrence would not differ substantially from other forms of conventional deterrence. However, some substantial differences exist due to the nature of cyber space. Three problems stand out in particular: the problem of attribution; the problem of

whether and where to set thresholds for retaliation; and the problem of the proportional retaliatory threat.

19. In cyber space, it is very difficult to trace an intrusion back to the intruder and/or the instigator. This is the problem of attribution in cyber space. For one, most intrusions take place through third party networks, most famously through so-called ‘botnets’, i.e. through a network of computers owned by people who are unaware that their computers are used for malicious purposes. Also, even if an attack is traced to hackers in a certain country, it is very hard to establish a connection between them and the government – hackers do not need to be housed in barracks or wear uniforms. Often such a connection does not even exist. Instead, a cyber intrusion could be the deed of so-called ‘patriotic hackers’ who want to support their government, but are not acting on its behalf. One observer concludes, “[a]ttribution will be difficult or impossible if a perpetrator – either a state or an individual – uses new tools and techniques and leaves no clues; if the perpetrator maintains perfect operational security; if the perpetrator makes no demands; and, most important, if the hostile actions require a rapid response” (Lin, 2012). Others, including the US government, are optimistic that sufficient progress will be made on the attribution problem for deterrence to work. Furthermore, attribution might not be as critical a problem as many argue. The more severe a cyber-attack is, the more interest the attacker has in claiming responsibility for the attack (Rid, 2013). If the aim of an attack is to compel or coerce an adversary, attribution is necessary – for how can the victim give in to the opponent’s demands if the victim does not know who the opponent is? And if the attack is part of an ongoing armed conflict, then the victim most likely knows who the attacker is.

20. Another basic problem of cyber deterrence is whether or not to set thresholds for retaliatory action and, if yes, where to set them. Not all hostile cyber actions merit retaliation. In cases of cyber espionage for example, retaliatory action cannot credibly be threatened, since the international order does not prohibit spying on other states. If it is clear that a state is the victim of a cyber-attack, the question then becomes what amount and what kind of damage warrants retaliation. Can a threshold be set according to economic damage, physical damage to infrastructure, or the loss of human life, especially since such damage is only an indirect and sometimes unintended effect? At this point, no clear legal understanding exists on what would constitute the use of force by a cyber-attack or even an act of war. In the absence of such a clear understanding, how can one set a threshold for retaliation? And, if a threshold was set, could a potential adversary be encouraged to conduct cyber hostile actions just below the threshold, without fearing retaliation?

21. A third problem is the question of proportional retaliation. To begin with, should a country limit itself to retaliation in cyber space or should it retaliate in a different manner? Naturally, this depends on the gravity of the hostile act. However, if retaliation should take place in cyber space, can the victim credibly threaten the assets of the attacker (Libicki, 2009)? There is an abundance of hostile actors in cyber space, and since cyber retaliation needs to be tailored according to the gravity of the attack as well as their respective vulnerabilities, a great amount of efforts and resources are needed to build a credible deterrence posture. Moreover, even if a state in fact develops specific retaliatory measures, it is not clear that the aggressor would still be vulnerable at the time when retaliation would become necessary.

22. Cyber deterrence is neither straightforward nor easy and many further questions remain. Can states or organisations credibly extend cyber deterrence to allies? What acts of retaliation would lead to unintended escalation of the conflict? All of these questions will probably be answered in due time. After all, it took nuclear strategists roughly two decades to reach some fundamental understandings of what deterrence meant in the nuclear age. However, many experts suggest that, at this point in time, ‘strategic ambiguity’ and flexibility – about what actions triggers retaliation and what form retaliation takes – is the most workable cyber deterrence posture. However, as the number of hostile cyber actions mounts over time and deterrence is tested, such a position could become less tenable.

3. Cyber 'Arms' Control

23. Some form of arms control, for example through international norms and legal measures, could be a possible solution for mitigating the cyber threat to national security. However, cyber defence and deterrence are already beset with many unanswered questions and even more present themselves with regard to arms control. Indeed, the prospects to solve these questions and establish even rudimentary arms control appear slim for the moment (Lin, 2012). If one looks towards a restriction of research and development of malicious code, how would one verify that no state or non-state actor is developing such code? After all, it only takes one clever hacker with minimum equipment to write such code. Also, one of the most effective ways to discover flaws in networks is by penetration testing, where a ‘red team’ tries to overcome defences with malicious code. Forbidding such activity would mean that hostile actors gain a crucial advantage. If one looks towards restricting or outlawing the use of malicious codes by states in conflicts, would states be tempted to use them after all if they were engaged in a conflict where they were losing, and what would prevent non-state actors – for example terrorists or ‘patriotic hackers’ – from using them? If one were to look towards banning cyber espionage, this would go well beyond the current international regime, which does not consider spying as a prohibited activity. However, more serious research into cyber arms control could yield innovative approaches, enhancing the prospects of success. In the meantime, it could be worthwhile to reach a common understanding of cyber concepts. Also, signing agreements on cyber problems outside the realm of national security, for example on cybercrime, could lead to new avenues of cyber arms control. For the time being, however, states need to deal with a world where malicious code will continue to proliferate.

D. THE PROSPECT OF INTERSTATE CYBER CONFLICT

24. Given the current vulnerabilities of military networks and critical infrastructure, combined with the fact that offensive cyber capabilities proliferating widely, is there a real possibility for interstate cyber war? Despite much hyperbole in the public at times, there are good reasons to be sceptical.

25. First, cyber weapons inflict physical damage – to hardware, infrastructure, or people, for example - only indirectly by leading to system failure. Indeed, until now, malicious code has only led to three known cases of physical damage and none of them caused any harm to human life: in the 2007 Aurora laboratory experiment where a generator was badly damaged; in the Stuxnet sabotage where Iranian centrifuges were destroyed; and in the 2012 Shamoon sabotage against Saudi Aramco which caused major damage to its business network (but notably not to its oil and gas infrastructure). Second, cyber-attacks need to be highly tailored to a specific target, making cyber weapons unlikely to be deployed in wide-area attacks. Third, once a cyber weapon is launched, it is highly unlikely that it can be used to the same effect. In fact, it is more likely that it will be blocked, as the victim adapts to the malicious code. Fourth, even though the value of a particular code diminishes for an attacker after having used it, other actors, either the victim itself or third parties, can modify the sophisticated code and use it against the attacker. Fifth, once unleashed, a cyber weapon could spin out of control, hitting targets unintentionally, perhaps even targets in the attacking state.

26. For all of these reasons, most analysts today agree that cyber weapons are unlikely to cause catastrophic damage at a moment’s notice, and thus produce strategic effects like, for example, a disarming nuclear strike. That is not to say that cyber weapons will not find a place in war and warfare, but it does mean that “cyber power should be understood as just another category of weapon” (Gray, 2013). The prospects for cyber terrorism should not be underestimated, but even here scepticism is warranted, as terrorists traditionally aim for highly visible and emotional attacks, which are hard to achieve with cyber weapons. For states, cyber weapons do have unique advantages: they can achieve military aims faster, over a longer range, and in a cheaper, less risky and more stealthily fashion (Gray, 2013; Bockel, 2012). Military experts argue that likely role

for cyber-attacks would be as enablers of military actions, especially in surprise attacks which could lead to operational success, for example at the start of a wider armed conflict, or in special operations (Libicki, 2009). Many legal scholars and governments also do not believe that cyber weapons pose fundamental challenges to the law of armed conflict, although it needs to be interpreted for cyber-attacks. In sum, as two observers conclude, “the correct frame of reference for Information Age conflict is not ‘pure play’ state-on-state ‘cyberwar’ in which strategic objectives may be met through cyber *coups de main* on their own. The correct frame is ‘cyber-skirmish’, a more or less constant hum of low-level activity over a wide ‘virtual landscape’, often conducted by irregular actors, with few or no single engagements of strategic consequence, however weighty in aggregate the stakes may be” (Betz and Stevens, 2011).

III. EURO-ATLANTIC DEFENSIVE RESPONSES

27. Given the potential impact and global proliferation of cyber threats, Euro-Atlantic states are looking to establish and bolster cyber security policy and practices at the national and multinational levels. Although cyber security has received sustained, high-level attention in recent years, countermeasures against cyber threats are still in developmental stages. To illustrate some of the cyber defence efforts undertaken, this section first examines the action taken by the United States, arguably the Euro-Atlantic leader in cyber security, and France, a NATO member state which until recently lagged behind the other big Allies, but has been redoubling its efforts to counter cyber threats. Next, it turns its eye towards the multinational level where the EU and NATO are at the forefront of policy development and implementation. Both organisations seek to establish comprehensive policies setting clear standards for network security and emphasise the importance of co-operation between national governments and private industry. Key differences between EU and NATO cyber security policies are largely due to different organisational roles rather than divergent approaches to cybersecurity: NATO, for its part, owns its computer networks and systems, while the responsibilities for cyber security in the EU rest mainly in the hands of member states (Robinson, 2013).

28. Given that offensive cyber doctrines and rules of engagement are secret, this section does not specifically discuss offensive cyber capabilities. Both the United States and France have said that they possess offensive cyber capabilities; NATO and the EU, as international organisations, do not. Furthermore, this section also omits detailed discussions on specific cyber arms control steps. For a number of reasons, the United States and the EU as a whole do not advocate formal rules on cyber arms control, but support discussions on confidence-building measures, norms and rules of the road in this respect.

A. THE UNITED STATES

29. The 2010 National Security Strategy identifies cybersecurity threats “as one of the most serious national security, public safety, and economic challenges” faced by the United States (US White House, 2010). US cybersecurity strategy is directed toward two main goals: improving resilience to cyber incidents and reducing the cyber threat. Achieving the former involves hardening digital infrastructure, improving methods of defence, and supporting quick recoveries from cyber incidents. Achieving the latter involves “working with allies on international norms of acceptable behaviour in cyberspace, strengthening law enforcement capabilities against cybercrime, and deterring potential adversaries from taking advantage of […] remaining vulnerabilities”.

30. From an organisational standpoint, the responsibility to protect digital infrastructure in the United States is split between the Department of Defense (DoD), which secures military networks, and the Department of Homeland Security (DHS), which secures civilian government networks and co-operates with private entities.

31. Within the DoD, cyber space mission responsibilities are assigned to US Cyber Command (USCYBERCOM). USCYBERCOM is co-located with the National Security Agency (NSA), the organisation responsible for US signals intelligence. Indeed, the Director of the NSA is ‘dual-hatted’ as the Commander of USCYBERCOM. The command is tasked with synchronising and co-ordinating cyber efforts within the different branches of the US military. Generally speaking, the DoD is concerned with three areas of hostile cyber actions: theft or exploitation of data; disruption or denial of access or service of networks and systems; and destructive cyber action.

32. The DoD cyber policy is currently guided by the 2011 Strategy for Operating Cyber Space. It lays out the strategic context of the cyber threat and proposes five strategic initiatives:

- Treat cyberspace as an operational domain to organise, train, and equip so that DoD can take full advantage of cyberspace’s potential networks and systems
- Employ new defence operating concepts to protect DoD networks and systems
- Partner with other U.S. government departments and agencies and the private sector to enable a whole-of-government cybersecurity strategy
- Build robust relationships with U.S. allies and international partners to strengthen collective cybersecurity
- Leverage the nation’s ingenuity through an exceptional cyber workforce and rapid technological innovation

33. The protection of critical infrastructure from cyber threats in the United States has fallen to the responsibility of the executive branch, as Congress has failed to pass any major cyber security legislation since 2002. DHS is the primary government agency tasked with critical infrastructure protection, including protection from cyber threats. Given the vast number of owners and operators of critical infrastructure, both public and private, the role played by DHS is quite broad. Specifically, DHS provides “strategic guidance to public and private partners, promotes a national unity of effort, and co-ordinates the overall Federal effort to promote the security and resilience of the nation’s critical infrastructure” (US Department of Homeland Security).

34. Within DHS, the cyber security aspects of critical infrastructure protection are co-ordinated by the National Cybersecurity and Communications Integration Center (NCCIC). The NCCIC mission emphasises co-operation and information sharing between all levels of government and the private sector. Its activities include the provision of situational awareness regarding vulnerabilities, intrusions, incidents, mitigation, and data recovery actions. For example, the NCCIC manages the United States Computer Emergency Readiness Team, which responds to cyber incidents, provides technical assistance to operators, and disseminates notifications about current and potential threats. Although NCCIC works closely with critical infrastructure owners and operators, it has no authority to enforce compliance with cybersecurity measures on the private sector.

35. Beyond the role played by the DHS, a 2013 Executive Order issued by President Obama to improve the cybersecurity of critical infrastructure tasked the National Institute of Standards and Technology with creating a cyber security framework. The institute completed the national cybersecurity framework in February 2014. It amounts to a set of voluntary minimum standards offering benchmarks on cyber defences for private operators. The framework may serve as the basis for future regulation on a sector-by-sector basis. Indeed, federal agencies are currently tasked with an evaluation of existing cyber rules for the industries under their purview, with the possibility of creating regulatory standards (Romm, 2014). Strict implementation of the framework across all critical infrastructure sectors is unlikely without Congressional action, but DHS, and the Departments of Commerce and the Treasury are reviewing incentives packages that could induce private sector compliance (Selyukh, 2014).

36. The United States has emphasised international collaboration as a first principle for developing cyber policy. Hence, it published its International Strategy for Cyber Space in 2011. Its

main goal is to work for "an open, interoperable, secure, and reliable information and communications infrastructure" by creating "an environment in which norms of responsible behaviour guide states' actions, sustain partnerships, and support the rule of law in cyberspace."

B. FRANCE

37. Cyber security emerged as a distinct national security priority in France's 2008 White Paper on Defence and National Security. Since then, France has steadily improved its cyber defence and security policies and has further intensified its efforts under the current Defence Minister Jean-Yves Le Drian.

38. In 2009, France established the French Network and Information Security Agency (ANSSI) under the authority of the Secretary General for Defence and National Security (SGDSN). ANSSI is, at present, the national authority for the defence of information networks and systems in both public and private sectors. The surveillance, analysis, and response to attacks on military systems are the responsibility of the Analysis Centre for Defensive Cyber Operations (CALID), which is now housed in the same premises. ANSSI's mission is four-fold (ANSSI, 2013):

- "To detect and early react to cyber-attacks, thanks to the creation of a strong operational center for cyber defence, working round-the-clock and being in charge of the continuous surveillance of sensitive Governmental networks, as well as the implementation of appropriate defence mechanisms;
- To prevent threats by supporting the development of trusted products and services for Governmental entities and economic actors;
- To provide reliable advice and support to Governmental entities and operators of Critical Infrastructure;
- To keep companies and the general public informed about information security threats and the related means of protection through an active communication policy".

39. ANSSI's objective to provide advice and support to operators of critical infrastructure is well supported by its overall mission. Information sharing, research and development, and risk assessment are key aspects of an effective public-private partnership in cybersecurity. These efforts represent the foundation of France's cyber security strategy, and the government is intent on further guaranteeing the protection of its critical infrastructure.

40. Increasingly the target of cyber espionage operations, France seeks to strengthen its cyber defence capabilities in attack prevention, detection, and resilience. In service of these goals, the 2013 White Paper on Defence and National Security highlights state support of high-level scientific and technological expertise, control over security system supply chains and service providers, reinforced intelligence capabilities, and co-operation with trusted international partners. Implementation of such measures is fast-moving, as the government is clearly motivated by a sense of urgency. In February 2014, Defence Minister Le Drian announced a 1 billion euro Cyber Defence Pact (*Pacte Défense Cyber*). It has six major goals:

- Heighten the level of security of the Ministry's information systems and means of defence and intervention, as well as those of its major trusted partners
- Prepare for the future by intensifying research efforts in the technical, academic and operational fields while supporting the industrial base
- Strengthen human resources assigned to cyber defence and build related career paths
- Develop the Cyber defence Centre of Excellence in Brittany for the Ministry of Defence and the national cyber defence community
- Cultivate a network of foreign partners in Europe, within the Atlantic Alliance and in areas of strategic interest
- Further the emergence of a national cyber defence community based on a circle of partners and the reserve networks

41. One of the concrete actions that comes out of the Cyber Defence Pact is that the personnel at the cyber defence expertise centre in Bretagne will be almost doubled (from 250 to about 450) over the next few years. This brings the personnel dedicated to cyber excellence more closely in line with other European players in cyber defence.

42. The 2013 White Paper on Defence and National Security also seeks to update and strengthen France's cyber defence in the realm of critical infrastructure protection as the state seeks to establish centralised regulation. In reference to the information systems of critical infrastructure operators, the White Paper asserts, "the state will define the security standards to be met with respect to IT threats by means of an appropriate legislative and regulatory procedure, and will ensure that operators adopt all necessary measures to detect and handle any such incident affective their sensitive systems" (French Republic, 2013). Thus, France recently passed in the Military Planning Law (*loi de programmation militaire)* for 2014-2020 explicit legislation on standards for cybersecurity, especially for government networks and private critical infrastructure operators. The White Paper states that such legislation "will specify the rights and obligations of public and private actors, particularly in relation to audits, the mapping of their information systems, notification of incidents and the capacity of the national agency responsible for the security of information systems (ANSSI), and, where applicable, of other state agencies, to intervene in the event of a serious crisis" (French Republic, 2013).

C. NATO

43. Cyber defence was first identified as an issue on NATO's political agenda at the 2002 Prague Summit and gained significant traction in the wake of the cyber-attacks against Estonia in 2007 and against Georgia in the context of the 2008 Georgia-Russia war. These attacks demonstrated the need to take measures to strengthen cyber defences across the Alliance; NATO's first formal NATO Policy on Cyber Defence was adopted in January 2008. It was revised in 2011, and the Alliance agreed on an associated Action Plan for implementation. Currently, the policy is once again under review in order to be updated for the 2014 NATO Summit in the United Kingdom. The principal focus of NATO policy is on the protection of the communication and information systems that are NATO-owned including its networks at headquarters, agencies, and missions abroad. To this end, NATO primarily seeks to improve attack prevention and resilience and to avoid duplication of efforts with national or multinational efforts. At the heart of its cyber defence efforts is the NATO Computer Incident Response Capability Technical Centre, which is currently being upgraded with an investment of 58 million euro. One of the main aims of the upgrade is to create two rapid reaction teams that would intervene on NATO networks under attack.

44. The Alliance recognises the global nature of cyber space and its associated threats and thus does not limit its Policy on Cyber Defence to the protection of NATO's networks alone. NATO is to a certain extent critically dependent on Allies' national information systems and networks, and it therefore works with Allies to develop minimum cyber defence requirements. Indeed, the development of cyber defence capabilities is in the process of being integrated into the NATO Defence Planning Process. Allied states' governments may implement NATO cyber defence policies or request NATO's assistance at their own discretion. NATO has also integrated cyber defence into numerous NATO exercises at all levels, including strategic and field exercises. In terms of response to cyber-attacks, NATO maintains 'strategic ambiguity' and flexibility on how to respond to different types of crises that include a cyber component. The Alliance carefully avoid the question how Allies' obligations under collective defence relate to cyber-attacks, in large part because it is not clear what kind of cyber-attack would constitute an armed attack covered under the Washington Treaty's Article 5. Under the ongoing review of the NATO Policy on Cyber Defence, the role of NATO during cyber incidents is being worked out. Two basic options have been put forward: support for the Allies in the event of cyber-attack or a reform of NATO governance, conferring cyber-command upon NATO. It appears more likely that NATO will

continue to play only a facilitating role in Alliance cyber defence and provide a framework for Allies' mutual assistance.

45. At the multinational level, NATO and individual Allies work with partners, international organisations, academia, as well as the private sector to promote complementarity and avoid duplication. The NATO-accredited Cooperative Cyber Defence Centre of Excellence (CCD-COE) in Tallinn, Estonia is a clear example of how co-operation between such actors occurs in practice. NATO-accredited centres of excellence are not part of the NATO command structure, but are international military organisations that support NATO. The CCD-COE focuses on education, research, and development, aiming to be the main source of expertise in the field of co-operative cyber defence in the Alliance and in its partnerships. Indeed, on the invitation of the CCD-COE, an international group of experts the Tallinn Manual on the International Law Applicable to Cyber Warfare, the most exhaustive open-source study of the subject. The manual is set to be followed by a second volume to explain "what options governments have, under international law, to respond to cyber-attacks from other countries" (Hale, 2014).

46. Where NATO's role in cyber defence and the protection of military networks is clear, its role in defending critical infrastructure from cyber threats is not fully defined. As an intergovernmental politico-military alliance, NATO does not have a mandate to direct civilian or private infrastructures. NATO's cyber defence strategy stresses the importance of working with Allies to develop minimum cyber defence requirements respecting national critical information systems and networks. However, beyond assistance in hardening those critical information systems and networks, NATO does not have an established strategy for the protection of critical infrastructure. However, the Alliance recognises the gravity of the potential consequences of a co-ordinated cyberattack against critical infrastructure and is exploring how it may play a part in defending such infrastructure. NATO's 2012 Emerging Security Challenges in Europe conference, for example, concluded that "NATO must join the discussion on how to assess critical vulnerabilities, conduct training and education as well as understand and prevent threats together with other stakeholders" (NATO Emerging Security Challenges Division, 2012, p. 34). While the CCD-COE in Tallinn is doing meaningful work in these areas, NATO itself remains in the preliminary stages of thinking about a role in defending critical infrastructure from cyber threats. Many European Allies consider that some critical sectors are already under EU regulation.

D. THE EUROPEAN UNION

47. The European Commission, together with the High Representative of the Union for Foreign Affairs and Security Policy, published on 7 February 2013 a cyber security strategy for the EU. The cyber security strategy, entitled *An Open, Safe, and Secure Cyberspace*, applies to both public and private networks and is designed to "safeguard an online environment providing the highest possible freedom and security for the benefit of everyone" (European Commission, 2013a). The strategy acknowledges that, "it is predominantly the task of Member States to deal with security challenges in cyberspace" and proposes a variety of actions and policy tools involving EU institutions, member states, and private industry to improve overall EU performance. The EU's vision of cybersecurity is articulated in terms of the following five priorities:

- achieving cyber resilience
- drastically reducing cyber crime
- developing cyber defence policy and capabilities related to the Common Security and Defence Policy (CSDP)
- developing the industrial and technological resources for cyber security
- establishing a coherent international cyber space policy for the European Union and promoting core EU values

48. While only one of the five cybersecurity priorities listed above is specifically tailored to defence, it is understood that because cyber threats are often multifaceted, "synergies between

civilian and military approaches in protecting critical cyber assets should be enhanced". Ultimately, the EU is in the initial stages of developing and implementing a comprehensive cyber security strategy. However, EU efforts will be considerably strengthened in 2014, as the European Council in 2013 called for the development of an EU Cyber Defence Policy Framework, which is to be prepared by the High Representative the Union for Foreign Affairs and Security Policy, in co-operation with the Commission and the European Defence Agency (EDA). The aims of this framework are:

- "the development of Member States' cyber defence capabilities, research and technologies through the development and implementation of a comprehensive roadmap for strengthening cyber defence capabilities;
- the reinforced protection of communication networks supporting CSDP structures, missions and operations;
- the mainstreaming of cyber security into EU crisis management; raising awareness through improved training, education and exercise opportunities for the Member States;
- synergies with wider EU cyber policies and all relevant other actors and agencies in Europe such as the EU Agency for Network and Information Security;
- to co-operate with relevant international partners, notably with NATO, as appropriate"

49. EU policy relating to the defence of member states' networks associated with national security and military institutions is thus framed as a collaborative effort between national governments and the EDA co-ordinated under the CSDP. The EU has, however, acknowledged that, "a particularly serious cyber incident or attack could constitute sufficient ground for a Member State to invoke the EU Solidarity Clause".

50. The EU also seeks to reduce the vulnerabilities of critical infrastructure and increase their resilience in order to limit, as much as possible, "the detrimental effects of disruptions on the society and citizens" (European Commission (DG Home Affairs), 2013). Critical infrastructure protection is thus directed against all threats and hazards – one of which is cyber threat. The August 2013 Commission Staff Working Document on a New Approach to the European Programme for Critical Infrastructure Protection streamlines existing policy in three areas: prevention, preparedness, and response. The document identifies the EU Cybersecurity Strategy as the source of "actions that will further contribute to the cyber resilience and security of infrastructures covered by [the European Programme for Critical Infrastructure Protection]" (European Commission, 2013b).

51. EU-level organisations like the European Network and Information Security Agency (ENISA) and the Computer Emergency Response Team for the EU institutions (CERT-EU) exist to co-ordinate and support national-level activities. Broadly speaking, the EU seeks to provide member states with a forum for exchanging information and best practices on cybersecurity through ENISA and assistance in responding to a breach of cybersecurity through CERT-EU.

IV. CONCLUSION

52. Cyber threats to national security are a grave concern to all countries that rely heavily on computer networks and systems. Most serious forms of cybercrime, terrorism, espionage, sabotage, and even attacks by state actors will become a basic feature of the future strategic environment. Cyber capabilities will be included into all military endeavours. These challenges add an entirely new level of complexity to the management of international security. However, these challenges are not as insurmountable as some claim, provided that governments, owners and operators of critical infrastructure undertake all necessary efforts. Good cyber defences need to be the bedrock of national strategies. Without a good defence, cyber deterrence and potentially cyber arms control will not work. Deterrence and arms control in the cyber age still present policy makers with a lot of open and difficult questions. These will need to be answered to stabilise cyber security

efforts. Indeed, for individual states the priority should be to concentrate on cyber defences first, and only when they have reached sustainable levels should, if they wish, turn to offensive cyber capabilities and arms control.

53. Cyber security efforts are, first of all, a national responsibility that states need to live up to. This is especially true in an alliance, as cyber threats know no boundaries. Cyber threats against one NATO country could undermine the Alliance as a whole. However, as national efforts are ongoing, international co-operation, especially within NATO and the EU, adds substantial unexplored and untapped value. In 2014, both NATO and the EU will therefore develop cyber defence strategies that will help to improve our collective as well as individual security. At this point in time, it would be premature, however, to shift more competences to NATO or the EU. For one, many national cyber defences are still lacking behind their peers, but more importantly co-operation on matters of cyber defence is still particularly complex because cyber security is a new aspect of national defence policy. Deeper co-operation should only take place when national authorities have understood the cyber threat and developed internally coherent policies. It would therefore be better if states were more incentivised to increase their cyber defences for the good of all. NATO, EU and national strategies need to be co-ordinated closely, to avoid duplication of efforts, but also because it is indeed difficult to co-ordinate strategy on an issue that often transcends national and regional borders. Your Rapporteur will monitor the efforts taking place in Europe and North America, both at the national and international level, over the course of 2014 and update the report accordingly. The cyber threat is here to stay, and lawmakers of the Alliance need to understand the complexities behind the huge challenge of incorporating cyber defence into our national and international defence policies.

BIBLIOGRAPHY

ANSSI, *Mission*, 2013, http://www.ssi.gouv.fr/en/the-anssi/mission/

Betz, David J and Tim Stevens, "Chapter Three: Cyberspace and War", *Adelphi Series*, no. 51, 2011

Bockel, Jean-Marie, "Rapport d'information fait au nom de la commission des affaires étrangères, de la défense et des forces armées (1) sur la cyberdéfense", *Rapport du Sénat de la République Française*, no. 681, 2012

Chen, Thomas M, *An Assessment of the Department of Defense Strategy for Operating in Cyberspace*, Carlisle: U.S. Army War College Press, 2013

CSIS/McAfee, The Economic Impact of Cybercrime and Cyber Espionage, CSIS, 2013, http://www.mcafee.com/sg/resources/reports/rp-economic-impact-cybercrime.pdf

European Commission (DG Home Affairs), *Critical Infrastructure*, 29 November 2013, http://ec.europa.eu/dgs/home-affairs/what-we-do/policies/crisis-and-terrorism/critical-infrastructure/index_en.htm

European Commission, *Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace*, JOIN(2013) 1 Final, 2013a

European Commission, *On a New Approach to the European Programme for Critical Infrastructure Protection Making European Critical Infrastructures More Secure*, SWD(2013) 318 final, 2013b

Farwell, James P and Rafal Rohozinski, "The New Reality of Cyber War", *Survival*, vol. 54, no. 4, 2012

French Republic, *French White Paper on Defence and National Security*, 2013, http://www.rpfrance-otan.org/IMG/pdf/White_paper_on_defense_2013.pdf

Gray, Colin S, *Making Strategic Sense of Cyber Power: Why the Sky is not Falling*, Carlisle: U.S. Army War College Press, 2013

Hale, Julian, "NATO-backed Project Explores Legal Options to Respond to Cyberattacks," Defense News, 23 January 2014, http://www.defensenews.com/article/20140123/DEFREG04/301230033/NATO-backed-Project-Explores-Legal-Options-Respond-Cyberattacks

Kuehl, Daniel F, "From Cyberspace to Cyberpower: Defining the Problem," in Kramer, Franklin D, Stuart H Starr, and Larry K Wentz (eds.), *Cyberpower and National Security*, Washington, DC: National Defense University Press, 2009

Libicki, Martin C, *Cyberdeterrence and Cyberwar*, Santa Monica: RAND Corporation, 2009

Lin, Herbert S, "A Virtual Necessity: Some Modest Steps Toward Greater Cybersecurity", *Bulletin of the Atomic Scientists*, vol. 68, no. 5, 2012

Lin, Herbert S, "Offensive Cyber Operations and the Use of Force", *Journal of National Security Law & Policy*, vol. 4, no. 63, 2010

NATO Emerging Security Challenges Division, *The World in 2020 – Can NATO Protect Us*, 2012, http://lgdata.s3-website-us-east-1.amazonaws.com/docs/1494/764045/ESC_Conference_2012_12_10_FINAL.pdf

Rid, Thomas, "Cyber War will not take place", Oxford University Press, 2013

Robinson, Neil, "Tangled Web: Cybersecurity Strategies Raise Hopes of International Cooperation," *RAND Review*, Summer 2013

Romm, Tony, "Cybersecurity in Slow Lane One Year after Obama Order," *Politico*, 9 February 2014, http://www.politico.com/story/2014/02/cybersecurity-in-slow-lane-one-year-after-obama-order-103307.html

Selyukh, Alina, "U.S. to Offer Companies Broad Standards to Improve Cybersecurity," *Reuters*, 12 February 2014, http://www.reuters.com/article/2014/02/12/us-usa-cybersecurity-standards-idUSBREA1B0AL20140212

US Department of Defense, *Department of Defense Strategy for Operating in Cyberspace*, 2011, http://www.defense.gov/news/d20110714cyber.pdf

US Department of Homeland Security, *Critical Infrastructure Security*, n.d., https://www.dhs.gov/topic/critical-infrastructure-security

US White House, *2010 National Security Strategy*, 2010, http://www.whitehouse.gov/sites/default/files/rss_viewer/national_security_strategy.pdf