DCAF Geneva Centre for Security Sector Governance

# INTRODUCTION TO CYBERSECURITY GOVERNANCE – A TOOL FOR MEMBERS OF PARLIAMENT

# INTRODUCTION TO CYBERSECURITY GOVERNANCE – A TOOL FOR MEMBERS OF PARLIAMENT


## Authors

### Franziska Klopfer

Franziska is a Project Coordinator in the Europe and Central Asia Division at DCAF.

### Irina Rizmal

Irina is a Project Officer in the Europe and Central Asia Division at DCAF.

### Milan Sekuloski

Milan is a Senior Advisor in the Europe and Central Asia Division at DCAF.

### Teresa Hatzl

Teresa is a former Project Officer in the Public-Private Partnership Division at DCAF.

### Dragan Mladenovic, PhD

Dragan is an expert in cybersecurity and cyber defence.

# Table of Contents

## Introduction

Cybersecurity is one of the latest aspects of national security policies that has become increasingly important throughout the security sectors of European countries. Policy makers are still catching up with the pace of technological developments utilised by a myriad of actors, both friendly and hostile. This requires new legal and policy frameworks to be developed quickly and comprehensively. Apart from ensuring national security, safe and secure networks are also important for boosting the national economy and modernising public sector governance in SEE countries (consider, for example, the crucial importance of a safe network for the good functioning of the e-governance services being introduced). A safe cyberspace is also necessary to ensure that citizens can exercise their rights, such as access to information and freedom of expression. Being aware of the opportunities, risks and threats cyberspace brings to the table is therefore of crucial importance.

Members of parliaments play a vital role in developing legislative and institutional cyber security frameworks, as well as in guaranteeing that principles of good governance apply in cybersecurity. As it comes with the responsibility of passing new legislation, they also have the power to convene different stakeholders for policy discussions, ensuring comprehensive, multistakeholder governance models – something that is especially important in cybersecurity. Finally, members of parliament also fulfil a watchdog role, overseeing the implementation of laws and policies on (or related to) cybersecurity.

Bearing these responsibilities in mind, it is therefore of immense importance to keep members of parliament up to speed with the latest developments in cybersecurity, equipping them with adequate knowledge and understanding to tackle policy issues and debates from an informed standpoint. This publication seeks to provide those members of parliaments who are engaged in legislative development and oversight of cybersecurity issues with a baseline overview of the main issues, trends and governance challenges.

This introduction, a Tool for members of parliament, explains the main elements of cybersecurity and its governance: cybercrime, cyberwar, cyberterrorism, cyberespionage and hacktivism and the challenges and opportunities in governing them. Each section is complemented with a list of possible questions that members of parliament can raise in relation to the issue. The questions aim to increase government accountability and that of other key cybersecurity stakeholders. They can be included in questions to the government, discussed in public hearings or inspire parliamentary inquires.

# SECTION I – KEY CONCEPTS

## Cybersecurity Needs, Policy and Strategic Goals

With the advent of the World Wide Web and the increasing move to a life online, it has become necessary to re-evaluate security risks and the responses to them. The current information age has pushed information and cybersecurity to the forefront as an important

aspect of individual, organisational, national, and international security. According to an ISO/IEC standard, cybersecurity represents the "preservation of confidentiality, integrity, and availability of information", among other properties.

In the concept of good security sector governance, security policy aims to ensure not only the security of the state but also the security of the individual. Applying this approach to the online world means that cybersecurity should strive to create a safe online space for all. To achieve this, cybersecurity policy must span across a number of issues, ranging from protecting the integrity of the state and ensuring people's human rights, to enforcing the law and preventing crimes committed in, or through, cyberspace. Matters of cybersecurity governance should therefore not only address issues of maintaining online security and resilience, but also of building safety and fostering opportunities online.

A first step in devising successful cybersecurity policy and strategy is therefore to define security objectives and set out what maintaining security and building safety online means for the country and its citizens. Critical assets that are fundamental for protecting the normal functioning of the state, as well as the general integrity of life online need to be defined. Electricity grids and key internet services are obvious examples of critical assets that require significant attention and protection. At the same time, the main factors of vulnerabilities in cybersecurity come from human error and technical failures. Uninformed internet users who click on the wrong link are the most frequent causes of cyber incidents. Education and awareness-raising of users is therefore equally as important for prevention in cybersecurity as is sound technology and the right experts to use this technology.

## Challenges in Cybersecurity Governance

Once cybersecurity objectives are defined, a governance framework has to be set in place, which determines the roles and responsibilities of different actors in achieving the objectives. A crucial challenge in cybersecurity governance is the fact that the roles and responsibilities of different actors are not yet clearly defined in international law or standards. Many national legal and policy frameworks also do not yet clearly reflect the influence of different actors. For example, who controls and who is responsible for a secure infrastructure or for safe online content? What duties or privileges stem from this responsibility?

Many essential cybersecurity services are owned and run by private actors while the state depends on their active cooperation, for example in securing their own networks and services. Cooperation between, and engagement of, different stakeholders is therefore essential for effective and efficient cybersecurity and for ensuring that cybersecurity policy-making is participative and accountable. For example, it is increasingly common for private and public actors to share information in order to better prevent and detect cyber incidents. At the same time, many private companies often have more advanced technology and expertise than the public sector and could share these means in an effort to increase the overall cybersecurity of the country, ultimately making their own businesses more secure. Finally,

all cybersecurity stakeholders – the government, the legislator, the private sector, civil society, the technical community and academia – have a role to play in the cybersecurity policy process, whether it would be in contributing to policy planning, cooperating in policy implementation or overseeing the entire policy process.

However, the exact extent of the responsibilities and the roles that these stakeholders should play has to be defined in each policy context. Overall, the credibility and implementation of the entire process relies on its inclusivity and transparency.

## A New Notion of Security Provision, Control and Oversight

Cybersecurity needs to be accountable. Control and oversight mechanisms often lack clarity due to the complex blend of state and non-state actors involved. As a result, new models not only of cooperation but also of control and oversight need to be developed.

Members of Parliament should play an important role in the oversight of cybersecurity governance. Because cybersecurity touches not only on security policy but also on other policy areas, cybersecurity oversight should bring together members of security and defence committees with committees in charge of telecommunication, education, information society and human rights, to name but a few.

## Examples of Questions for Oversight:

- Does the country have a cybersecurity strategy with a clearly defined vision? What ministry or state agency is responsible for its implementation? Was the strategy developed through an inclusive process, engaging all relevant stakeholders (state and non-state)?
- Is there a list of identified critical information infrastructure and, if so, is this list exhaustive? What state agency is responsible to keep this list up-to-date? Who is responsible for controlling the protection of critical information infrastructure?
- Who are the different cybersecurity actors? What are their roles? What should be their responsibilities?
- Are there control and oversight mechanisms for key state and non-state cybersecurity actors in place? Is the control and oversight of key state and non-state cybersecurity actors working? Are they being held to account to ensure that their activities are not only effective but also within the limits of the law?

# SECTION II – CYBERCRIME

## Definition

Cybercrime is generally understood as criminal acts in which computers and networks are the main target, are employed as tools to commit an offence, or are the location of the crime.

Although there is no universally accepted definition, a distinction between two main types of cybercrime can be made:

- Cyber-enabled crime, referring to 'traditional' forms of crime now transferred into the cyber sphere, such as financial-focused criminal acts, acts that impede on the safety of children and young adults, and even terrorism; and
- Advanced cybercrime (also known as high-tech crime), referring to sophisticated attacks against computer hardware and software.

First, it is important not to confuse cybercrime with cybersecurity. The two cyber-related threats differ in motive, intent, tools employed, target, scope, consequences as well as actors engaged in prevention and mitigation. In practice, cybercrime varies from spam and phishing emails, online scams and fraud, and false representation, to prohibited offensive and illegal content, identity theft, and online child sexual abuse material. The main motivation behind cybercriminal acts, as in the case of 'traditional' crime, is generally seen as financial gain. Cyber criminals are, in essence, hackers with malicious intent.

## Computer and Networks as the Main Target

When it comes to the tools most commonly employed, these include malicious software such as viruses, Trojan horses, adware and spyware for gaining access to systems, monitoring activities and collecting data; botnets, or hijacked personal computers that remotely perform tasks without their users' knowledge; and Denial of Service (DoS) attacks aimed at exhausting the resources available to a network, application or service, in order to prevent users from accessing them.

The effects of such attacks are also multi-faceted. Private individuals can suffer financial loss, but also fall victim to personal and sensitive information as well as identity theft. Companies that fall victim to cybercriminal attacks face potential financial loss, as well as loss of sensitive operational information, data on patents or personal data of their clients and users, all of which can also indirectly carry severe reputational consequences. Public institutions or non-commercial organisations can become victims of extortion or of theft of personal data of users of their services.

## Computers and Networks as Tools to Commit an Offence

Further criminal acts also spreading into the cyber sphere include the illicit trade of drugs, weapons and sensitive data and information, human trafficking and even contract killings, beatings and other forms of violence. In general, such arrangements take place on the so-called **'darknet'** where users can act in complete anonymity. Using the darknet, individuals and criminal organisations make use of encrypted messaging services to communicate, and cryptocurrencies to carry out financial transactions, making tracking and identification extremely challenging. Black-hat hackers (criminals with technical skills, or technical experts employed by the criminals, see chapter on hacktivism) also utilise the potential of the darknet by capitalising on the software vulnerabilities they have detected, anonymously selling them to anyone looking for ways to exploit specific systems.

## Computers and Networks as the Location of a Crime

Criminal groups have thus made an extremely efficient transition into the digital sphere. They have even developed new business models that resemble some of the most advanced legitimate businesses. Just as some companies offer 'security as a service' and develop the cybersecurity capacities of interested buyers, criminal groups also offer 'crime as a service' on the cybercriminal market. Another concern is the possible cooperation between different malicious actors. For example, cybercriminals could offer their services to terrorist groups or carry out state-sponsored criminal acts in cyberspace solely for the purpose of financial gain. In other words, the digital sphere offers criminal groups new outlets and opportunities to carry out illicit activities that otherwise may not have been available.

## Trends and Responses to Cybercrime

Overall, cyber-enabled crime is in steep rise both in developed and developing countries. By its very nature, cybercrime is international and exceeds national borders. The perpetrators need not be in the same country as the victims or the police forces pursuing them. This poses one of the key challenges in the fight against cybercrime, as differences in legal systems and practices of the various countries involved may affect the efficiency and feasibility of cooperation, as well as the exchange of intelligence and evidence.

Furthermore, very few police forces in the world have the capacity to tackle cybercrime incidents independently even though many of them have dedicated cybercrime or 'high-tech crime' units. As with other types of malicious activities in cyberspace (see chapter on cyber espionage), there is an obvious asymmetry of costs involved. As a result, the traditional approach to policing crimes is somewhat altered in the cyber sphere. Instead of arresting perpetrators immediately, police cybercrime units focus primarily on discontinuing ongoing criminal acts and addressing the security vulnerabilities that have been exploited. With the challenge of attribution equally present across the cyber spectrum and the lengthy and

demanding process of investigation, including data forensics, arriving at official verdicts also comes at a slower pace than with traditional crimes.

At the national level, the fight against cybercrime requires all actors to cooperate. The private sector is the most common target of cybercriminals and its experiences and interests should be taken into account when planning cybercrime strategies. Cybercrime experts from the private sector, as well as academia and civil society can also contribute to cybercrime policy planning with technical capacity and knowledge. To tackle cybercrime efficiently, governments therefore must foster public-private cooperation and support the establishment of networks of trust. Equally important is cybercrime prevention and the support to individual users. Through general awareness raising and capacity building users should learn to recognise potential fraudulent emails, malicious content as well as potentially deceitful contacts. Even relatively small efforts like teaching users to maintain basic cyber hygiene and use strong passwords, up-to-date licensed software and encryption, can have a great impact in preventing cybercrime.

At the international level, progress has been made with the adoption of the Council of Europe Convention on Cybercrime, also referred to as the Budapest Convention. The Budapest Convention is the only binding international instrument on cybercrime to date, providing guidelines to countries for developing comprehensive national legislative frameworks to fight cybercrime and establishing a framework for international cooperation between signatory states. With sixty-one parties and another ten expected to join, the Budapest Convention, however, is still not a universal global document. Nevertheless, instances of international collaboration can be observed in recent years. For instance, international police cooperation organisations, most notably Europol and Interpol, have engaged in efforts aimed at enhancing international capacities and the facilitation of cross-border cooperation frameworks among police services. With the previously mentioned high demands of maintaining comprehensive national cybercrime units, such frameworks may compensate for limited national capacities, including through the development of public-private partnerships and trust networks between experts from different sectors of society.

## Examples of Questions for Oversight:

- Does the country have legislation on cybercrime, identifying different types of cybercrime and establishing a well-defined sanctioning system? To what extent is it aligned with the international conventions the country is party to?
- Are the judiciary and police well equipped in terms of technical knowledge, expertise and capabilities?
- Which parts of society are most exposed to cybercrime? Are any preventive initiatives aimed at those sectors in place?

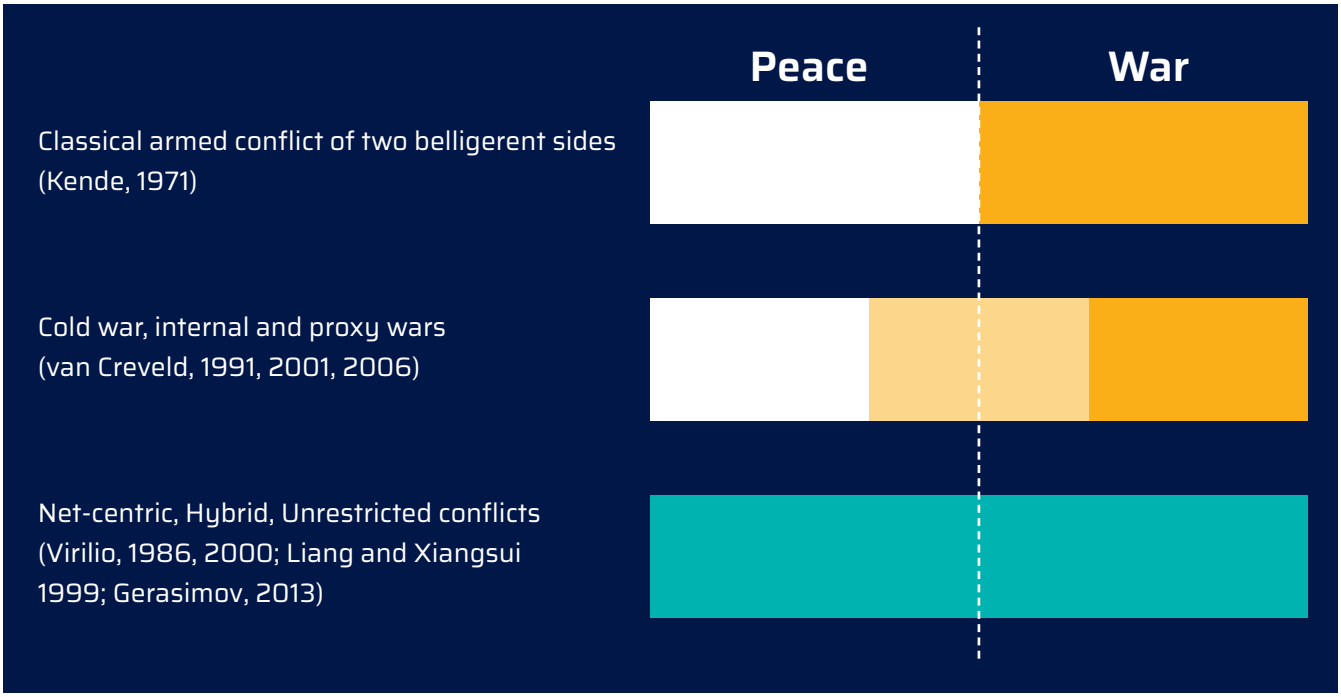
- Is the control and oversight of key state and non-state actors working? Are the cyber capabilities of the security agencies being held to account to ensure that their activities are not only effective but also within the limits of the law/not violating guaranteed citizens' rights to privacy?
- Are the police and judiciary using all available legal tools for effective international cooperation? Should legislative frameworks change to facilitate better efficiency? At the same time, what safeguards are there for the protection of citizens' personal data shared with third countries? Is the communication with the private sector efficient and transparent (in its form, if not in the content which should be classified)?

# SECTION III – CYBERWAR

## Definition

Cyber warfare can be defined as the act of „waging war in cyberspace or through cyberspace". It is a new, specific type of warfare which uses information communication technologies (ICT) to achieve military objectives and effects in the physical, information and cyber domains. The military effects can be identical to the effects of kinetic, nuclear, biological or chemical arms.

However, there is no international agreement on how the content, methods, techniques, means, and goals of cyber warfare should be defined. The international community has also not yet agreed on how to develop national capacity building measures and international confidence building measures, or on how to apply existing international law to cyber warfare.



## Problems in Regulating Cyber Conflict

New technologies with offensive capabilities emerge faster than individual countries are able to develop the necessary defences against them. They also outpace the ability of the international community to find solutions for regulating cyber conflicts.

The perpetrators of cyber-attacks often operate in a clandestine manner, with the effects of their cyber-attacks in many cases delayed. Several years can pass between the cyber exploitation and installation of a malicious weapon and the discovery of its effects. The attackers can be government units and agencies, as well as private companies, criminal organizations, terrorists or informal groups and individuals.

In contrast to conventional warfare, the effects of cyber conflicts often do not reach the threshold of an "act of aggression"[1], "use of force"[2], "armed force"[3] or "armed attack"[4] as defined by the UN Charter, making it difficult to apply ius ad bellum and ius in bello rules of the International Law of Armed Conflicts.

Indeed, most states do not have sufficient capabilities to:

- accurately detect cyber-attacks;
- identify and attribute attackers; and
- timely, accurately and legally respond to cyber-attacks.

## International Efforts in Regulating Cyber Warfare

Lack of legal regulation leaves space for potential abuse of cyber-attacks possibly even leading to outbreaks of international and regional crises, especially in regions burdened with chronic political tensions.

The international community is still trying to establish an agreement on ways to regulate cyber warfare. There are different proposals, one of which is the Tallinn Manual[5], developed by a group of scholars at the NATO Cooperative Cyber Defence Centre of Excellence in Tallinn, Estonia.

---

1 Charter of the United Nations. 24 October 1945. United Nations. 1 UNTS XVI, art 39.
2 Ibid., 1 UNTS XVI, art. 2, para. 4.
3 Ibid., 1 UNTS XVI, Preamble.
4 Ibid., 1 UNTS XVI, art. 51.
5 Schmitt, Michael N. (ed.) 2017. Tallinn Manual 2.0 on the international law applicable to cyber operations. Cambridge University Press.

## International Legal Responses to Cyberwar

A possible practical response to cyber threats can be the adoption and application of capacity and confidence building measures at national, regional, and international level.

To this end, the United Nations assembled the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security (UN GGE). The Group has convened five times in the period between 2004 and 2017 to deliberate on existing and potential threats; norms, rules, and principles of responsible state behaviour; and confidence and capacity building measures. In the 2013 Report, the GGE concluded that „International law, and in particular the Charter of the United Nations, is applicable and is essential to maintaining peace and stability and promoting an open, secure, peaceful and accessible ICT environment".[6]

Additional efforts are made by Organization for Security and Co-operation in Europe (OSCE), through the adoption of Confidence building measures for preserving international peace and stability (CBMs).[7] The CBMs focus on information exchange and dialogue; protecting critical infrastructures and national security; and promoting and improving public-private cooperation.

Both of these initiatives, however, are voluntary (non-obligatory for UN or OSCE member States) and their existence is not an outright, firm guarantee for achieving peace and security in cyberspace at international level.

A possible solution can be bilateral and multilateral agreements between different states. These agreements can define norms, standards, and principles of peaceful behaviour; establish rules and procedures in cases of severe cyber incidents; facilitate collaboration and creation of common capacities for cyber-attack detection, attacker identification and attribution.

## Examples of Questions for Oversight:

- Are strategic goals for cyber defence defined?
- Is there a situational awareness assessment? Does it take into account all of the elements in the country that need protection?

[6] Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security. 24 June 2013. UN General Assembly. Resolution A/68/98.

[7] Decision No.1106. Initial set of OSCE Confidence-Building Measures to reduce the risks of conflict stemming from the use of Information and Communication Technologies. 3.12.2013. Organisation for Security and Cooperation in Europe. PC.DEC/1106. Decision No.1202. OSCE Confidence-Building Measures to reduce the risks of conflict stemming from the use of Information and Communication Technologies. 10.3.2016. Organisation for Security and Cooperation in Europe. PC.DEC/1202.

- What are the main vulnerabilities and risks? Are they regularly identified, revised and addressed?
- How developed are existing national capacities for cyber defence?
- Who are the different actors, nationally and internationally, that contribute to cyber defence?
- What frameworks are there in place for cooperation among responsible actors? How are these organised and how accountable, transparent and effective are they?
- Is the frequency and scope of training provided for responsible staff sufficient?
- Does the country take part in regional and international trainings and exercises? How often are do these take place?

# SECTION IV – CYBER ESPIONAGE

## Definition

Cyber espionage is defined as an act undertaken secretively or under false pretences that uses cyber capabilities to gather (or attempt to gather) information with the intention of communicating it to an opposing party.[8] Access is gained either by the individual posing as a legitimate user, or through the use of sophisticated, targeted attacks (such as social engineering) through which legitimate users are manipulated in a way that opens the door for individuals seeking to gain illegitimate access.

## Specific Challenges of Cyber Espionage

One of the core characteristics of cyber espionage is the sole asymmetry of the costs it implies. The costs of protecting and defending against all vulnerabilities are disproportionately high compared to the costs on the attacker's side, who needs to discover and exploit one single vulnerability. Furthermore, taking into account the time needed to detect an intrusion, cyber espionage poses as an effective offensive tool for obtaining information on systems, processes and individuals. Estimates of the time needed to detect a breach vary from one to three months[9], by which time the intruder can gain access to a large variety of sensitive information. With the extent of internet and online service penetration into societies across the world, cyber espionage opens much wider possibilities for gaining sensitive information on an adversary.

8 According to the Tallinn Manual referred to above.

9 The Mandiant Report (2013) estimates that the average time that access was maintained to a victim's network is 356 days. Global Space (2013) estimates that an average breach remains undetected on average for 90 days. Foreign Policy (2015) estimates that on average it takes a victim to detect that they have been infected is 205 days. Ponemon Institute (2015) found that breaches go undetected for 46 days on average. Kreps, Fletcher and Griffiths (2016) estimate that a breach remains undetected on average for 3 months.

## Acceptable Behaviour, Cybercrime or Act of Aggression?

There is increasing agreement that cyber espionage is generally becoming untenable. However, deciding what constitutes acceptable behaviour and what should be sanctioned is still a significant challenge. The fact that traditional espionage by countries has been treated as acceptable state behaviour in the past has left present-day cyber espionage unregulated as well. Consequently, in practice, mere intrusion into a computer system, violating its confidentiality, is still considered as acceptable. Violations of a system's integrity or availability, however, which may occur as a result of this intrusion, are considered as a form of cyber-attack and deemed unacceptable. Normatively, cyber espionage is therefore seen both as acceptable and unacceptable, depending on its consequences.

In addition, there is the challenge of differing between information gathering activities and those with malicious intent that can pose as acts of aggression. Again, this also depends on the use the information obtained is put towards. Therefore, there is a thin line between acts whose primary purpose is cyber espionage and those to be considered as outright cyber-attacks. This makes it extremely difficult to establish international principles and regimes governing the notion of cyber espionage which, for the time being, remains rather unregulated.

From a security aspect, cyber espionage is seen as potentially overlapping with notions of cybercrime. In this sense, cyber criminals can be contracted by third actors to perform and/or enable acts of cyber espionage, tasked with penetrating government and/or corporate systems and extracting sensitive information.

## Proxy Actors, Private Armies and Hybrid Conflicts

Another challenge is the issue of state-sponsored cyber espionage campaigns, whereby states can indirectly sponsor actors who have the capacity to penetrate their adversary's systems. In this sense, hackers have become potential private armies of spies in the digital age, at the disposal to the highest bidder. The rise of cyber espionage has also added another element to the developing notion of hybrid conflicts and asymmetric warfare, whereby conflicts are no longer black and white, but come in various forms and intensity. By engaging in cyber espionage, states are now able to develop hybrid relations with their adversaries. This means that, in effect, relations in the physical world are continued normally, while hostilities and conflicts take place in the digital domain, through the practice of cyber espionage, alongside hacking and hacktivism, cybercrime, and cyber offensive activities.

As with other forms of defence and protection against malicious activities in cyberspace, cyber espionage carries the challenge of detection and attribution. In addition, cyber espionage is not necessarily performed by states or state-sponsored actors. It can also be employed as a tool by cyber criminals, hacktivists as well as private actors to simply gain an economic advantage.

## Addressing, Regulating and Countering Cyber Espionage

The best defence strategy against cyber espionage is therefore – for the time being at least – that of deterrence. This implies increasing the actual or projected costs of a potential attack for the adversary. Alongside building stronger defences this also means promoting bilateral and multilateral cooperation on reaching agreements and/or codes of conduct that regulate the notion of cyber espionage, alongside other types of behaviour in cyberspace. A seemingly successful example of this is the 2015 U.S. – China agreement concerning economic espionage, which determines that neither country will conduct or knowingly support cyber-enabled theft of intellectual property with the intent of providing competitive advantages to companies or commercial sectors.

Cyber espionage to obtain intelligence for the purpose of national security, however, just as traditional forms of espionage, remains unregulated. For this reason, state-led initiatives see a rise in debates concerning the right to 'backfire', or hack-back once intrusion into a system is detected, as a more convincing form of deterrence. Among the latest countries to join these debates is Germany, where the national intelligence community is requesting to be granted the right to employ active defence. This would imply jurisdiction to destroy data stolen and relocated from German servers, as well as to compromise foreign servers in order to strengthen national surveillance capabilities. The idea behind such initiatives is to deter potential attackers by threatening retaliation.

## Examples of Questions for Oversight:

- What is being done to protect citizens and their data from cyber espionage? What ministries or state agencies are responsible for countering cyber espionage?
- Is there an assessment of the country's cyber espionage vulnerabilities and needs and what counter measures have been taken?
- How can cyber espionage be better defined and regulated by national legislation and at international level?

# SECTION IV – CYBER TERRORISM

## Definition

Cyber terrorism combines two of the world's most prominent developments: society's increasing reliance on the Internet and the threat of international terrorism.[10] The Internet's anonymous, easily accessible and often unregulated nature makes it particularly prone for exploitation and misuse by terrorist organizations and other non-state actors. However, while

[10] Lentz, Christopher E. Lentz. 2010. A State's Duty to Prevent and Respond to Cyberterrorist Acts. Chicago Journal of International Law 10. No. 2.

the use of the Internet for terrorist purposes constitutes a challenge for the international community, it also provides new means for counter-terrorism.

## Cyber Terrorism vs. the Use of the Internet for Terrorist Purposes

While there is no universally agreed upon definition of cyber terrorism, most national definitions refer to an attack which uses electronic means to penetrate and/or seriously interfere with national critical infrastructure.[11] The Organization for Security and Co-operation in Europe (OSCE) for instance defines cyber terrorism as "cyber-related terrorism and more specifically, [...], as terrorist attacks on cyber infrastructure particularly on control systems for non-nuclear critical energy infrastructure".[12]

Threat scenarios of cyber terrorism include paralyzing major urban areas, the public health sector or disrupting the financial sector by "changing a few ones and zeros".[13] The rise of the Internet of Things[14] constitutes another major insecurity that can be easily exploited by terrorist organizations to commit acts of cyber terrorism. Acts of cyber terrorism that will have an actual physically destructive impact are considered less likely and hence, less of a challenge to states, because of the immense amount of resources required to commit such an act.[15]

Moreover, many terrorist organizations use the Internet to commit traditional offenses, such as fraud, illegal access to and unlawful interference with computer systems. This results in an overlap between cybercrime (see chapter on cybercrime), cyber-attacks (see chapter on cyberwar) and cyber terrorism; eventually, making it difficult to differentiate between these. The United Nations Security Council Resolution 1566 might offer some guidance on this, as it underlines the politically motivated element, identifying "terrorist acts" as:

> "[...] criminal acts, including against civilians, committed with the intent to cause death or serious bodily injury, or taking hostages, with the purpose to provoke a state of terror [...], intimidate a population or compel a government or an international organization to do or to abstain from doing any act, which constitute offences within the scope of and as defined in international conventions and protocols relating to terrorism [...]."[16]

11 National critical infrastructure is an asset or system vital for the maintenance of essential societal functions and, which, if taken offline for an extended period, would create a serious risk to public health, the economy, the environment, citizens and national security.

12 Good Practice Guide on Non-Nuclear Critical Energy Infrastructure Protection (NNCEIP) from Terrorist Attacks Focusing on Threats Emanating from Cyberspace. 2013. Organization for Security and Co-operation in Europe. No.16.

13 Gen. Votel, Joseph L.. July 2015. Understanding Terrorism Today and Tomorrow. CTC Sentinel 8. Issue 7, pp.2–6.

14 Cambridge Dictionary defines "Internet of Things" as the objects with computing devices in them that are able to connect to each other and exchange data using the Internet. The Internet of Things is increasingly embedded in national critical infrastructure.

15 Weimann, Gabriel. March 2004. https://www.usip.org/publications/2004/03/wwwterrornet-how-modern-terrorism-uses-internetwww.terror.net:%20How%20Modern%20Terrorism%20Uses%20the%20Internet. Special Report No.116.Untied States Institute of Peace.

16 Security Council resolution 1566 (2004) on Threats to international peace and security caused by terrorist acts. 8 October 2004. United Nations Security Council. Resolution S/RES/1566. Op. para. 3.

In addition, terrorist organizations use the Internet on a daily basis for a range of activities, such as propaganda (including radicalization, incitement to terrorism, recruitment), financing, training, and planning (including through secret communication and open-source information), as well as to carry out cyber-attacks.[17] While the use of the Internet for propaganda purposes has gained high prominence within the international community, calling for stronger partnerships, including with the tech industry,[18] the challenge of using the Internet for financing purposes has been very often disregarded. Meanwhile, the general shift towards the use of technology in international commerce has transformed the Internet into an asset for terrorist organizations to launder money, raise and transfer funds.[19]

Consequently, law enforcement and intelligence service agencies are increasingly monitoring suspicious online financial transfers and are developing tools and skills to proactively prevent, detect and respond to terrorist activity involving the Internet. Governments have also started to respond to the use of the Internet for propaganda purposes through strategic communications, such as alternative narratives and counter-messaging, and content regulation.[20] However, any counter-terrorism activity on the Internet prerequisites concerted efforts between States, the private sector and civil society to effectively respond to these new challenges.

## Rule of Law Consideration

In general, counter-terrorism activities involving the Internet may have an impact on a number of human rights (including privacy and freedoms of expression, association, peaceful assembly, and religion or belief). With regard to the use of the Internet for propaganda purposes, Governments have adopted new measures, ranging from repudiating attempts at the justification or glorification (apologie) of terrorist acts to prohibiting by law the incitement to commit these.[21] However, it should be noted that speech that is morally repugnant, shocks, disturbs or offends does not per se rise to a criminal level; but "[s]uch are the demands of that pluralism, tolerance and broadmindedness without which there is no 'democratic society'."[22] However, the challenge is to identify the tipping point at which contestation or criticism turns into hate speech, glorification (apologie) of, or incitement to commit terrorist acts. Identifying this tipping point is not always straightforward.

In essence, it is important that Governments clearly define relevant offences in their national criminal codes, in order to allow citizens to foresee consequences coupled to

17 See: The Use of the Internet for Terrorist Purposes. 2012. United Nations Office on Drugs and Crime.

18 See: SC Counter-Terrorism Committee; Tech Against Terrorism; Global Internet Forum to Counter Terrorism.

19 Jacobson, Michael. June 2009. Terrorist Financing on the internet. CTC Sentinel 2. Issue 6, pp.17–20.

20 See: Zurich-London Recommendations on Preventing and Countering Violent Extremism and Terrorism Online. 2017. Global Counterterrorism Forum.

21 See Countering Terrorist Narratives. 2017. United Nations Security Council. S /RES/2354 (2017). Preambular para. 12. And Prohibition of incitement to commit terrorist acts. 2005. United Nations Security Council. S/RES/1624 (2005). Preambular para. 4 and Operative para. 1(a).

22 Handyside v. The United Kingdom. 4 November 1976. Council of Europe: European Court of Human Rights. 5493/72, op. cit., para 49

certain actions, and avoid over-regulation and hence a "chilling-effect" on human rights. Due process guarantees, such as the presumption of innocence and the right to a fair trial, are essential in ensuring that counter-terrorism measures are effective and respect the rule of law. Moreover, effective oversight of the public security actors involved in counter-terrorism (online and offline) is crucial for promoting human-rights compliant reform processes in counter-terrorism.

### Examples of Questions for Oversight:

- Is there a clear legal framework in place, identifying prohibited acts on the Internet?
- Are the right to freedom of expression and the right not to be subjected to arbitrary or unlawful interference with one's privacy guaranteed in the Constitution?
- Does any parliamentary committee have the legal mandate to oversee the work of state's agencies responsible for counter-terrorism?
- Is the legislation regulating counter-terrorism activities on the Internet, observing the human rights standards? Is legislation adopted following a public and inclusive consultation process?
- What possibilities are there for Parliament to scrutinize private companies regarding their practices on the collection of personal information of their users?

# SECTION V – HACKTIVISM

## Definition

By definition, hacktivism is a blend of hacking and traditional activism. The term itself has not been assumed by 'hacktivists' themselves, but rather attributed by researchers, journalists and cybersecurity professionals within attempts at distinguishing between different actors in cyberspace. Hacktivism enables new forms of mobilisation for online activists in their fight for a specific cause (e.g. human rights, freedom of speech, etc.). It thus enables remote action and large-scale mobilisation at a click of a mouse. In terms of consequences, mere hacktivism in general causes minor damage, which is why very few cases reach the point of actual prosecution, especially given the additional challenge of attribution equally present here as within any other type of activity in cyberspace.

## Motives of Hacktivists and Difference to Cybercrime and Cyber Terrorism

Crucially, hacktivism is seen as disruptive, rather than destructive. This is what distinguishes it from other form of malevolent activities in cyberspace, such as cybercrime or cyber terrorism.

Hacktivists mainly rely on tactics such as spreading worms and viruses, Distributed Denial of Service (DDoS) attacks, web defacement, and the like. The extent to which hacktivists are generally seen as a minor threat is portrayed by the common characterisation of their DDoS attacks being equal to the 1960s sit-in form of protest.

Hacktivists, however, also engage in activities such as taking over Twitter accounts and Facebook pages, as well as stealing and/or disclosing sensitive and personal information from and on the systems they penetrate.

## White, Grey and Black Hat Hackers

Given that hacktivists are, in essence, hackers with a cause, the specific actions they take upon penetrating a system distinguish between different types of hackers. These are:

White hat hackers are those who upon discovering vulnerabilities in systems report these to the system's developers in order for targeted patches to be developed and overall security of the system improved. White hat hackers are also described as 'ethical hackers'.

Grey hat hackers also report discovered vulnerabilities to the system's developers but may ask for financial remuneration or some other form of reward for the information they provided.

Black hat hackers do not report detected vulnerabilities to the system's developers and instead look to gain from these either through direct exploitation or through selling this information on the black market to other actors, such as cyber criminals.

There is a very thin line between hacktivism and actual offensive activity in cyberspace. Hacktivists, in some cases, may cooperate with cyber criminals. Additionally, direct public threats made by certain hacktivist groups towards various governments, enterprises and individuals can potentially entice panic and fear among civilian populations, one of the core elements of the definition of terrorism. Finally, recent debates have seen an increase of references made to the notion of state-sponsored hacktivism, which, although reasonable assumptions on its existence can be made, is in practice virtually impossible to prove.

## Examples of Questions for Oversight:

- What are the capacities of law enforcement to identify hacktivism and differentiate it from other forms of cyber threats? Are they sufficient?
- Does the relevant legislation clearly define which activities included in the term 'hacktivism' are illegal (i.e. when they cross the line of free speech)?

- What can be done by the government to support 'white hat hackers' or to avoid confounding them with 'grey' or 'black hat hackers'? Are any of the whistle-blowers' protection mechanisms applicable to 'white hat hackers'?
- What is being done to identify potential hacktivists and prevent criminal behaviour? Are there legal and operational safeguards for preventing security services from misusing authority and undermining/disabling legitimate activism?
- What is being done to increase international cooperation on countering malicious hacktivism?

DCAF Geneva Centre for Security Sector Governance

**DCAF Geneva**
P.O. Box 1360
CH-1211 Geneva 1
Switzerland
Tel: +41 (22) 730 94 00
Email: info@dcaf.ch

**DCAF Brussels**
/ EU SSG Facility
24 Avenue des Arts (boîte 8)
1000 Brussels
Belgium

**DCAF Ljubljana**
Gospodinjska ulica 8
1000 Ljubljana
Slovenia

**DCAF Ramallah**
Al-Maaref Street 34
Ramallah / Al-Bireh
West Bank, Palestine

**DCAF Beirut**
Gefinor Bloc C
Office 604, Ras Beirut
Lebanon

**DCAF Tunis**
Rue Ibn Zohr 14
1082 Tunis
Tunisia