WEBINAR SERIES
TRAINING SUMMARIES

JUNE 2015

GCCS2015 WEBINAR SERIES

GCCS2015
COLLATED TRAINING SUMMARIES

Global Partners Digital
Development House
56–64 Leonard Street
London
EC2A 4LT
+44 (0)207549 0337

gp-digital.org

CONTENTS

INTRODUCTION

The Government of The Netherlands hosted the fourth Global Conference on Cyberspace (GCCS2015) on 16-17 April 2015. Following on from the London (2011), Budapest (2012), and Seoul (2013) Conferences - a series also known as the London Process, the 2015 event in The Hague provided an opportunity for further high-level discussion of key cyberspace issues, structured around the three main themes of Freedom, Security and Growth. The Conference was a stock-taking event, assessing the current global situation and mapping out the challenges and opportunities that lie ahead.

Based on the assumption that all those who have a stake in cyberspace should be able to express their views and participate in a meaningful way, the GCCS2015 organisers put particular emphasis on facilitating multistakeholder engagement in the Conference, welcoming almost 300 civil society participants alongside an equal number of government and private sector representatives.

As part of the effort to facilitate effective civil society engagement in GCCS2015, a tailor-made training program for civil society, organised by the GCCS Advisory Board, under the leadership of Tim Maurer and in partnership with the Government of the Netherlands, was delivered through a series of seven webinars open to the public in the run up to the Conference, accompanied by written summaries for each. These webinars were delivered by experts in the field and mirrored the agenda of the main Conference, allowing participants to gain a wider understanding of the cybersecurity and human rights issues that were addressed there.

Each webinar consisted of a 30-minute presentation, followed by a 30 minute Q&A session where participants were able to interact with the speaker. The webinar recordings and training materials were then used as the foundation for a 1.5 day civil society Pre-Event to the Conference, which aimed to familiarise a targeted group of participants with the main issues on the Conference agenda as well as the broader cybersecurity debates.

This booklet contains the summaries for each webinar. You can find the webinar recordings and presentations at: gp-digital.org/publication/gccs2015.

01

CYBERSECURITY AND HUMAN RIGHTS

CAROLINA ROSSINI AND NATALIE GREEN, PUBLIC KNOWLEDGE

EXECUTIVE SUMMARY

This will serve as an introduction to cybersecurity with a particular focus on the policy aspect of cyber security, including how cyber security is addressed in international relations and the impact cyber security has on human rights. By the end of the module, you should be able to answer the following questions:

- What role do "definitions" play in cybersecurity debates, discussions, and policy decisions?
- What are the main human rights concerns when dealing with cybersecurity?
- Are there international laws and standards that apply to cybersecurity? Do they address human rights concerns?
- How is cybersecurity addressed regionally and internationally?

BACKGROUND: HISTORY AND DEFINITIONS

Since the first computer worm was unleashed in the late 1980's to the recent 2014 Sony Pictures Entertainment hack, the security and stability of cyberspace, including the Internet, are often cornerstones from which discussions around cybersecurity, Internet governance, and Internet freedom begin. Threats to cybersecurity can include computer viruses, spam, identity theft, data breaches, denial of service attacks, and cybercrime. Attackers can range from hackers to activists to petty criminals to businesses to national governments. With over 370 million people falling victim to cybercrimes each year[1] and tens of thousands of known viruses in existence[2], the threats to our security are real - but so are the threats to our human rights online. Before looking at the human rights concerns in relation to cybersecurity, let's take a quick look at the outward expressions of cybersecurity.

In practice, outward expressions of cybersecurity include domestic public policy and laws (creation of cybersecurity agencies, such as the United States' Cyber Command), international public policy discussions (talks around creating an ITU/UN cybersecurity treaty), private business practices (anti-virus software, notification programs by ISPs, firewalls, etc), online surveillance (often by governments), and technical community practices aimed at maintaining the critical infrastructure of the Internet (Internet Engineering Task Force is one of these independent technical agencies).

1 http://www.pcmag.com/article2/0,2817,2425118,00.asp
2 https://www.uhd.edu/computing/helpdesk/documents/virusfacts.pdf

When talking about cybersecurity, what exactly do we mean? As you'll soon realise, there are a variety of definitions and terms that are used by cybersecurity firms, governments, international organisations, human rights activists, and others for different means, though they vary by a few words.

DEFINITIONS

In fact, a great example is the term cybersecurity itself, which the European Union defines as "safeguards and actions that can be used to protect the cyber domain, both in the civilian and military fields, from those threats that are associated with or that may harm its interdependent networks and information infrastructure"[3]. The ITU defines cybersecurity as "the collection of tools, policies, security concepts, security safeguards, guidelines, risk management approaches, actions, training, best practices, assurance and technologies that can be used to protect the cyber environment and organisation and user's assets"[4]. Another example is the definition developed by the Freedom Online Coalition's cybersecurity Working Group "An Internet Free and Secure" based on the ISO 27000 standard, "Cybersecurity is the preservation – through policy, technology, and education – of the availability, confidentiality and integrity of information and its underlying infrastructure so as to preserve the security of persons both online and offline."[5]

The Internet Society (ISOC) has pointed that cybersecurity is "a catchword" that is "frighteningly inexact and can stand for an almost endless list of different security concerns, technical challenges, and "solutions" ranging from the technical to the legislative. While buzzwords like cybersecurity may make for good headlines, serious discussions of security and the Internet require a shared understanding of what is meant by cybersecurity."

As compared to many other areas of international relations or Internet-related topics, there is a void of concrete internationally-agreed upon definitions for phrases and definitions used to discuss cybersecurity. The definitions of 'information security', 'cybersecurity,' 'cyber-warfare', 'cyber-surveillance' and many others have not been agreed upon in a binding, standard setting international body or agreement. That means these terms are used by different actors in different ways, thus making policy discussions more confusing and making it easier for some governments to violate basic rights in the name of a broad 'cybersecurity' threat. In 2014, the Swiss government funded a project to consolidate cybersecurity related definitions in the Global Cyber Definitions Database. Before you continue, use the database to look up the various definitions of each of the following, as these words are crucial to your understanding of the basics of cybersecurity:

- Cybersecurity
- Internet security
- Information security
- Critical infrastructure
- Cyber space
- Cybercrime
- Cyber warfare
- Cyber threat
- Hacktivism

3 http://ec.europa.eu/digital-agenda/en/news/eu-cybersecurity-plan-protect-open-internet-and-online-freedom-and-opportunity-cyber-security
4 http://www.itu.int/online/termite/index.html
5 https://www.freedomonlinecoalition.com/how-we-work/working-groups/working-group-1/

BRIEF OVERVIEW WHERE CYBERSECURITY IS BEING DISCUSSED

HOW CYBERSECURITY IS ADDRESSED AT THE NATIONAL LEVEL

Cybersecurity involves helping protect the information that you, me, governments, businesses, and others keep online or in cyberspace, including communications (email, video messaging), finances (credit card information on websites like Amazon or the account numbers and information you use for e-banking), personal data (social security number, medical records on healthcare website), military secrets, and much more. Cyber incidents can also cause physical damage to critical infrastructure and networks as evidenced by the Stuxnet malware discovered in 2010 that targeted and destroyed some of centrifuges at the Natanz nuclear facility in Iran.

It is under this backdrop that cybersecurity threats and the risk of cyber attacks that could leak confidential military secrets or damage a country's economic/political infrastructure have garnered large attention not just as an Internet-related issues, but also as a national security issue. Other examples of national security threats throughout the world include nuclear weapons proliferation and war.

The United States, Russia, Japan, Kenya, European Union countries, are among the many countries that have declared the issue of cybersecurity, and specifically cyber attacks against their governments and citizens as a national security threat and developed national **cybersecurity strategies or initiatives.** Such cybersecurity initiatives and strategies normally outline the country's primary goals, concerns, set of principles or norms, and actions to be taken related to cybersecurity. Initiatives also can set up the creation of new agencies to deal with cybersecurity domestically or outline the role of already existing agencies, such as law enforcement, military, defense and foreign affairs ministries, in implementing cybersecurity policies. Cybersecurity initiatives, such as the United States' also support the development of **public-private partnerships (PPPs)** between government agencies and private sector companies, such as Internet Service Providers (ISPs), critical infrastructure owners, and technical companies around implementing cybersecurity measures across sectors. While governments mostly create and develop the cybersecurity initiatives, they may also consult technical experts, private businesses, and civil society for recommendations on how to improve strategies.

In discussing cybersecurity, you will most often hear about cybersecurity laws and measures to defeat **cybercrime**. In general, cybercrime refers to crimes that take place with or deal with computers and cyberspace, but also to traditional acts of crime (such as drug trafficking) that take place online. Within many countries' national cybersecurity initiatives and strategies are specific references and initiatives towards combating cybercrime based off current law enforcement and criminal justice systems. As you'll see in the **Human Rights Concerns About Cybersecurity** section, governments and surveillance agencies alike often cite "combating cybercrime" as a reason to support overarching cybersecurity and cybercrime laws and practices.

CYBERSECURITY AT THE INTERNATIONAL LEVEL

While domestic laws and practices have been working to address cybersecurity concerns, the issue of cybersecurity is a truly transnational issue. Cyberspace is

a borderless series of networks, and cybersecurity threats move across military, political, and geographical boundaries. Attackers can be highly targeted or they can choose to unleash a threat that could impact dozens of countries and millions, or billions of people at once. As domestic initiatives, and countries without extensive cybersecurity plans, have failed to stop the growing number of highly sophisticated transnational viruses and threats, international cooperation around cybersecurity issues is becoming the focal point of civil society, governments, private sector, and others.

While some have pointed to international cooperation as the key to a secure Internet in the future, many countries have yet to set their own domestic policies that properly address cybersecurity, and other countries have adopted overarching policies that directly violate human rights. In fact, an often ignored factor in cybersecurity debates on the international scene is the role that states themselves play in exacerbating cybersecurity threats and concerns. The United States, European Union countries, Iran[6] , Israel [7], China, and Russia[8] have all been accused of launching cyber attacks against other states and of creating a 21st century arms race - the **cyber arms race.**

At the international organisation level, the issue of cybersecurity first came to the UN's agenda when the Russian Federation introduced a draft resolution in the First Committee of the UN General Assembly that was later adopted in 1998. Since 2010, three Groups of Governmental Experts (GCEs) have been tasked by the UN General Assembly to research and report on existing and potential threats to cybersecurity and recommendations on how to address them. In their 2010, 2011 and 2012/2013 reports, GCEs concluded, amongst a number of things, an increased need for "international cooperation against threats in the sphere of ICT security" with input from civil society and the private sector, but also emphasised that "State efforts to address the security of ICTs must go hand-in-hand with respect for human rights and fundamental freedoms set forth in the Universal Declaration of Human Rights and other international instruments." In 2014, the UN adopted a new resolution on cybersecurity, and it is expected that another GCE report, possibly influenced by revelations of United States and United Kingdom mass online surveillance, will be issued in 2015.

Another important move that was made at the UN was the letter sent by Russia, China, Uzbekistan, and Tajikistan to the UN Secretary-General calling for an International Code of Conduct for Information Security. Though the letter recognizes the role of human rights in cybersecurity, it also emphasises the need for states to curb "the dissemination of information that incites terrorism, secessionism, extremism, or undermines other countries' political, economic and social stability," a clause that is worrying to free expression advocates. The UN Institute for Disarmament Research, the UN Office on Drugs and Crime, the International Telecommunications Union, and the UN Human Rights Council have all made various statements and pushed for initiatives related to cybersecurity.

At the regional and bilateral level, almost every single world region has held policy discussions, and some have even issued treaties, on cybersecurity. Both the North Atlantic Treaty Organisation (NATO) and the Organisation for Security and Cooperation in Europe (OSCE) have adopted principles or tasked member states to build collaboration around cybersecurity issues such as, capacity building, cybercrime, and the applicability of international law (including human rights law) to cybersecurity. In 2013, the European Union (EU) adopted the Cyber Strategy of the European Union: An Open, Safe and Secure Cyberspace which emphasised

6 http://www.businessinsider.com/iran-is-officially-a-real-player-in-the-cyber-war-2014-12

7 http://f.cl.ly/items/0t073Y3i3P0v2o2x0q39/Baseline%20Review%202014%20ICT%20Processes%20colprint.pdf

8 http://www.computerworld.com/article/2532289/cybercrime-hacking/cyberattacks-knock-out-georgia-s-internet-presence.html

protecting freedom of expression and privacy in core cybersecurity principles, but also tasked a number of other bodies in Europe including the European Parliament, the European Network and Information Security Agency, and others to provide further assistance, information sharing, and training to EU member states.

To read more about these regional efforts including those in Asia, Africa, and Latin America and global bilateral efforts in cybersecurity, consider reading pg. 15-25 in "Baseline Review of ICT-Related Processes and Events."

Other than the conventions and decisions already mentioned, the issue of cybersecurity has become increasingly central within the spectrum of traditional multistakeholder and multilateral internet governance spaces. In summer 2013, the Internet governance community was shaken by Edward Snowden's revelations on US and UK mass surveillance, and the push for increased cooperation and shaming related to cybersecurity increased dramatically. As already mentioned, within months of the revelations, Brazil and Germany sponsored a resolution at the UN on "The Right to Privacy in the Digital Age," which was eventually adopted in 2014. In April 2014, Brazil hosted Netmundial, the Global Multistakeholder Meeting on the Future of Internet Governance. The non-binding outcome document that was created with civil society input called for international cybersecurity policy decisions to be held in multistakeholder fora with engagement from all interested parties, including civil society. While non-binding, the Netmundial outcome document has been a tool for governments and civil society who have pushed against international multilateral cybersecurity treaties and decision-making.

The International Telecommunication Union (ITU) is the multilateral UN agency tasked with issues related to information and communications technologies (ICTs). Every four years, the ITU hosts a plenipotentiary conference in which the 193 member states decide on the future of the organisation. This meeting is open only to member states and the delegation members that these states choose. After the UN-sponsored World Summit on the Information Society (WSIS) global events were held in 2003 in Geneva and 2005 in Tunis to allow people and stakeholders around the world to give their input on issues related to Internet access, security, and privacy, the ITU was granted a role in facilitating WSIS Action Line item c5 "Building Confidence and Security in the Use of ICTs". Governments such as Russia and China have been able to use this Action Item role to push for increased consolidation of cybersecurity issues within the ITU.

In 2007, the ITU adopted a Global Cybersecurity Agenda as a framework for international engagement between Member States on cybersecurity issues. Four of the ITU's resolutions (resolutions 130, 174, 179, and 181) relate to cybersecurity, and leading up to the 2014 ITU plenipotentiary conference held in Busan, South Korea, a number of country delegations, including Russia and Arab states, suggested modifications to the resolutions to increase the ITU's role in cybersecurity.

At the annual multistakeholder UN-sponsored Internet Governance Forum (IGF), an increasing number of workshops and discussions have focused on cybersecurity, but the non-binding, non-outcome based fora have not yet produced any positions or policy statements on cybersecurity-related issues. In addition to the IGF, the multi-stakeholder conference series first held in London in 2011, called the "London Conference on Cyberspace" was launched with support from the UK government. The conference is an opportunity for all interested stakeholders to engage in discussions and debates on cybersecurity issues, and has since been held in Hungary and South Korea. The 2015 conference was held in the Netherlands.

AN INTERNATIONAL TREATY ON CYBERSECURITY?

Leading up to the ITU's 2014's plenipotentiary conference, there was also discussion of a cybersecurity treaty being negotiated, but that never came to fruition. Even so, discussions of an international convention or treaty on cybersecurity with a focus on expanding the already existing 2001 Council of Europe Convention on Cybercrime (aka the Budapest Convention) have been raised throughout the world, especially post-ITU plenipotentiary[9] . The Budapest Convention, though focusing specifically on cybercrime and not all cybersecurity issues, has been ratified by 44 countries (mostly European, but also including Australia, the Dominican Republic, Japan, Mauritius, Panama, and the United States). The Budapest Convention's primary goal is to harmonise domestic criminal law to certain areas of cybercrime in order to create an international norm for enhanced cooperation on cyber crime. In the convention, illegal access and interception, data and system interference, misuse of devices, computer-related forgery and fraud, child pornography, and some instances related to copyright are considered cybercrime offenses.

Arguments in favour of creating a cybersecurity treaty, with remnants of the Budapest Convention, include that the creation of an Internet-specific treaty could lead to creating laws of cyberwar, similar to conventional war treaties that may restrict attacks against citizens or children. Others have claimed that the creation of a cybersecurity treaty would likely be closed to the public and civil society and become highly politicised in an international organisation, such as the U.N. There's also significant worry that an international treaty related to issues of security would not fully take into consideration human rights law or would make exceptions to human rights law. Unsurprisingly, the issue of *definitions* is especially relevant as many countries use terms such as *cybersecurity* and *information security* interchangeably or may define *attackers*, *hacktivists*, and other key words differently. The harmonisation of such terms could lead to the acceptance of broad cybersecurity terms that could be used to further violate basic human rights in the name of security.

That's why a variety of civil society groups, including the digital rights coalition Best Bits, actively petitioned against increasing the ITU's role in cybersecurity and the development of an international cybersecurity treaty. The ITU's role in cybersecurity is often rebuked by governments and civil society for a number of reasons including lack of technical-expertise at the ITU, the broad language of proposed cybersecurity treaty language, the number of other UN agencies and other fora (both multistakeholder and multilateral) that could address cybersecurity, and the lack of transparency and participation opportunities, especially for civil society. Others look at the debate of the ITU's role in cybersecurity as a part of ongoing cyber-related issues and attacks between countries, including the United States and Russia.

HUMAN RIGHTS CONCERNS ABOUT CYBERSECURITY

Though some domestic and international laws attempt to address human rights considerations in forming cybersecurity standards, the negative impact on human rights caused by overarching and broad cybersecurity laws and principles has become apparent to civil society advocates and others.

When talking about human rights, we are mostly referring to those rights

9 http://f.cl.ly/items/0t073Y3i3P0v2o2x0q39/Baseline%20Review%202014%20ICT%20Processes%20colprint.pdf

guaranteed under the United Nations' Universal Declaration of Human Rights (UDHR) and the International Covenant on Civil and Political Rights (ICCPR), including **freedom of expression, freedom of speech, the right to privacy, freedom of opinion,** and **freedom of association** as some of the most basic rights of all humans. In response to the creation of the Internet as a new platform for expressing basic human rights, the UN Special Rapporteur on Freedom of Opinion and Expression and free expression rapporteurs from Europe, Latin America, and Africa signed a joint declaration confirming that **"freedom of expression applies to the Internet"** in 2011. In July 2012 the UN Human Rights Council further confirmed that **"the same rights that people have offline must also be protected online,"** thus making the formerly mentioned human rights declarations of UDHR, ICCPR applicable to the Internet.

A number of cybersecurity laws and measures that have been taken by individual countries could have a negative impact on **online speech** and **freedom of expression** by directly infringing upon such rights or creating a chilling effect on the desire of people to express their rights. The Anti-Cyber Crime Law of Saudi Arabia and its vague clause on "protection of public interest, morals, and common values", have been used to crack down on online speech and freedom of expression by imprisoning bloggers and others for voicing different opinions, insulting public officials, or supporting forces other than the government in power. In 2012, the Philippines approved the Cyber Crime Prevention Act that addressed legitimate cybersecurity concerns, such as child pornography and spam, but also criminalised libel. Though the provision on libel was eventually dropped the following year, its original intentions were enough to worry Filipino activists and lawmakers into drafting a bill called Magna Carta for Philippine Internet Freedom in direct opposition to the law. In addition to cybersecurity laws developed by governments, firewalls developed by IT businesses and companies (with government support) can be used to block specific websites and content, leading to **online censorship.**

Just a week after the Charlie Hebdo attacks in Paris in early 2015, Prime Minister David Cameron announced his support to ban encrypted message services, such as Whatsapp, if British intelligence agencies were not given increased access to messages and user data. Cameron stressed the need for increased access to encrypted messages as a means to protect the UK from terrorist attacks. Banning encrypted message services could be seen as a violation of both the right to privacy and online anonymity in the name of national security, through cybersecurity and online surveillance. The **right to privacy** allows for all people to keep information about themselves out of the hands of those they don't want to have the information. **Online anonymity** is the right to say something online without having it be connected to your real identity, and both are important for maintaining the Internet as a platform for free expression[10] , especially for political or social dissenters or those who want to avoid harassment, imprisonment or worse. In 2013, the UN Special Rapporteur on Freedom of Opinion and Expression issued a report on the impact of surveillance on human rights, noting that "the use of an amorphous concept of national security to justify invasive limitations on the enjoyment of human rights is a serious concern."

In 2009, the UN Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism issued a report that stated that Article 17 of the International Covenant on Civil and Political Rights (ICCPR) which states that "no one shall be subjected to arbitrary or unlawful interference with his privacy" is actually "flexible enough to enable necessary, legitimate, and proportionate restrictions to the right to privacy," but only in cases where a law is already in place that outlines when privacy can be violated, when it protects the rights of others, and/or when is in line with necessary and proportionate principles. **Necessary and proportionate principles**, and similar terms are often used to distinguish how surveillance practices, including online

10 https://www.eff.org/issues/anonymity

surveillance, can be done within international laws and human rights-based principles, including with proper public oversight, due process, and a system for user notification.

In addition to freedom of expression, speech, privacy, and anonymity comes the issues of ethnically and religiously discriminatory practices and standards within cybersecurity laws in the West against Muslims and the validity of online protest, such as hacking, as a cybersecurity threat.

Though cybersecurity threats are real, the ability to communicate anonymously, voice disapproval, protest, and have discourse without fear of persecution is an important part of human rights that all people are guaranteed. While state based agencies and actors have control and access to the Internet and its data, some have claimed that checks and balances are needed, such as oversight committees, international laws, and internationally agreed upon definitions for key words.

ROLES OF STAKEHOLDERS IN CYBERSECURITY

In talking about the multilateral and multistakeholder ways in which cybersecurity is addressed, it is important to understand what role different stakeholders play in these discussions. Ideally, governments, the private sector, civil society, and the technical community would all play equal roles in creating and implementing cybersecurity policies and decisions, but realistically this isn't always the case.

Traditionally, governments play the primary role in creating the public policies and laws that regulate and determine cybersecurity measures domestically, sometimes with non-governmental input, but usually from private cybersecurity firms or industry. In addition, governments are also capable of launching and supporting cyberattacks of their own against other countries, and they are the only stakeholder guaranteed a say in the ITU and other international multilateral bodies. On the international stage, a handful of governments (previously mentioned) have pushed for increasing the role of governments and intergovernmental organisations in cybersecurity.

Private sector companies, including ISPs and the IT sector are crucial because of their role in creating and maintaining the technologies (computers, tablets, etc) on which cybersecurity issues arise. Governments often consult these companies when making public policy decisions in order to ensure that cybersecurity standards can be applied to various technologies. At the same time, the number of cybersecurity firms in the private sector is quickly growing, and they often profit from strict cybersecurity policies. Similar to private sector companies, the technical community has the technical expertise and understanding of the Internet and is often cited by governments when developing cybersecurity policies. The technical community, including the Internet Engineering Taskforce also works independent of governments and politically-motivated cybersecurity measures to help ensure the security of the Internet's critical infrastructure .[11]

Similar to other areas of Internet governance, civil society's role in cybersecurity has just begun to take off in recent years. On the one hand, civil society groups have pushed for further inclusion at international discussions and domestic policy-making meetings, but others are calling for civil society to create their own positive agenda for cybersecurity policy and norm making. Civil society has a unique role in being able to advocate for cybersecurity policies from a human rights-based approach. In 2011, CitizenLab developed a report outlining the possible role

11 See pg. 106: http://www.oecd.org/sti/ieconomy/cybersecurity%20policy%20making.pdf

for civil society in cybersecurity, and in 2013, the Association for Progressive Communications created a similar agenda. Both reports emphasise the importance of civil society in bringing to light human rights considerations in all cybersecurity-related discussions, but also address the need for civil society to call for evidence-based cybersecurity decisions and practices.

02

THE TECHNOLOGY BEHIND CYBERSECURITY

NIELS TEN OEVER, ARTICLE 19

INTRODUCTION

Security can be defined as a state of being free from danger or threat. This can only be achieved if one has a level of control over the environment in which one is operating. In terms of systems security this would mean that one has control over the processes that are executed on a specific system and one has clear permissions for different (sets of) users. So nothing or noone does something that is not expected. To have this level of control over a system, one needs to understand what processes are running on a system and what these processes do. One also needs to have the trust or understanding that these processes will not all of a sudden execute operations that you do not expect them to perform, and if they might behave out of the ordinary, these processes should not have access to essential resources or operations. So security is in large part about restrictions.

THE WHAT – WHAT IS THE TOPIC ABOUT?

There are generally three levels of concern: Software, hardware and users. Software are all the programs, applications and operating system(s) that are running on your device, these are practically machine readable instructions that are performed by the hardware. The hardware is all the physical elements that constitute a computer system.

Both software and hardware can contain vulnerabilities, undocumented ways that could enable third parties to have access to your computer, often in a way that is difficult to detect. There are intentional vulnerabilities, which are called 'backdoors', that enable third parties to have access to the system or execute specific task. But there are also many unintentional vulnerabilities, which can be mistakes by developers, or an implementation that was secure when it was programmed, but because of new developments isn't secure anymore. There is a lively market in undiscovered exploits, which are called zero-days[12]. These are called zero-days because it has been zero-days that the vulnerabilities are known by the public. This is why a good understanding of the hardware and software and the expected behaviour is important.

Finally users are a crucial part to cybersecurity. Users don't like to be limited and often work around security barriers that have been put in place. For users, security often feels like a hurdle, like using strong passwords and replacing them every

12 http://www.technologyreview.com/news/507971/welcome-to-the-malware-industrial-complex/

three months. So they write their passwords on post-its, or re-use the same login and password they might use for a webshop (with very low security standards).

You might think that this only happens to home computers, but unfortunately bad security practices can be found everywhere on the Internet, ranging from very big routers to systems that control power plants. What makes doing security on the open Internet so hard is that what is secure today, might be insecure tomorrow. Vulnerabilities in crucial parts of software are found everyday. As previously mentioned, there is a market for zero-days, where some of the main customers are governments. This new trend stimulates security researchers to not disclose the vulnerabilities to the developers of the software, but rather to keep it hidden, which in the long term leads to a more insecure biotope of software.

For many parts of civil infrastructure where the net is used, these systems are called Industrial Control Systems (ICS), the large implementation of this are Supervisory Control and Data Acquisition systems, SCADA in short. These are used to control water purification plants, oil pipelines, power plants, and much more. By using the Internet, these networks are exposing themselves to attackers, but on the other hand it provides for ease of use and allows for remote control and monitoring. And this is exactly where its weakness lies. By being connected to the Internet it allows for third parties to try to get access to the systems; to prevent this, the systems need to be carefully configured and regularly updated. Unfortunately this is often not the case; people are not upgrading their servers, weak passwords are being used and sometimes the systems can be accessed via the browser through an insecure connection. It is often the perception that when a system is in place, no further work is needed, but maintenance, monitoring, updates and upgrades are an essential part of having a secure environment. And here we're not even talking about advanced targeted attacks.

THE WHY – WHY IS THIS TOPIC IMPORTANT FROM A HUMAN RIGHTS PERSPECTIVE?

The issue of security becomes harder when we add Internet to the mix, because the system one tries to secure is much more exposed. To make a system more secure practically means to limit its possibilities: the fewer options there are, the fewer things can go wrong. But this is the opposite of what we want for the Internet, especially one that strengthens human rights: the Internet became the important infrastructure for freedom of expression and access to information that it is today because its use is not limited to certain things, its aim is connectivity, and the Internet Protocol is the tool to realise this. This opens the endless opportunity for innovation, and possibilities but also a lot of risks.

THE WHO – WHO ARE THE MAIN PLAYERS?

In the guidelines for secure operations of the Internet (RFC1281) the IETF states that the Internet is a voluntary network, operated on a collaborative basis, and that everyone on the network has their own role to play in security:

- **Users** are individually responsible for understanding and respecting the security policies of the systems and they have a responsibility to employ available security mechanisms and procedures for protecting their own data.
- **Computer and network service providers** are responsible for maintaining the security of the systems they operate. They are further responsible for

notifying users of their security policies and any changes to these policies.
- **Vendors and system developers** are responsible for providing systems which are sound and which embody adequate security controls

Responsibilities are found on every level, but these are guidelines which are not always followed up. Most cybersecurity risks are caused by badly administered systems. This means security updates that have not been done, bad password management, opening of e-mail attachments with viruses. Bad administration of systems allows for botnets to take over your computer to do an orchestrated attack on thousands of computers at the same time.

THE HOW – HOW IS THIS TOPIC BEING ADDRESSED?

The trade in zero-days, the development of malware, and the practice of weakening standards are no precision attacks on specific targets, as one might think. Once attacks are 'out in the wild' they often get copied and partially re-used, both when it's a 'trick' or a piece of software. Even if we look at one of the most advanced attacks we've seen in recent history, the Stuxnet worm, which was aimed at an Iranian power plant, made its way across the Internet to India, Iran, Indonesia and back to the US. Technology democratises: once a code or practice is out there, one cannot get it back. This is why the development of malware and the trade in zero-days (instead of informing the providers of the vulnerability) are both such dangerous practices, which might even backfire against the party that developed it.

There is a world to win when it comes to cybersecurity. There is an increasing cooperation in this field, but more can be done: governments could standardise and support penetration (vulnerability) tests of its own systems, those of important industry players and critical infrastructure and report security vulnerabilities to developers. Computer Emergency Readiness Teams (CERTs) and Computer Security Incident Response Teams (CSIRTs) could be strengthened, and knowledge on digital security and best practices should be mainstreamed, so that no one leaves their digital house, factory or government building with the keys in the door.

03

ROLES AND RESPONSIBILITIES OF DIFFERENT ACTORS IN CYBERSECURITY

DR. MYRIAM DUNN CAVELTY, HEAD OF THE NEW RISK RESEARCH UNIT
AT THE CENTER FOR SECURITY STUDIES, ETH ZURICH

INTRODUCTION

To continue to respond to cyber threats and other challenges of the digital age, international cooperation is indispensable. GCCS2015 aims to strengthen and extend international security alliances by involving all relevant stakeholders, including private sector actors and civil society groups, in the search for lasting solutions to current and future cyber challenges.

Understanding different expectations and positions (in various geographical contexts) is important for fruitful multistakeholder interaction. However, when looking at the complex issue of cybersecurity and related topics, what type of actors have traditionally had what kind of roles and responsibilities? How have expectations about them changed over the years? And what would an optimal distribution of responsibilities look like from a civil society perspective? From many possible focal points, this webinar will pick the area of cybersecurity as its main case study. In the Q&A section, there will be time to discuss the particularities of other cyber issue areas if the participants wish to do so.

THE WHAT – WHAT IS THE TOPIC ABOUT?

Cyberspace is a domain decisively shaped by non-state (private) actors. This has important implications for cybersecurity: In contrast to many other security issues, private actors are not the ones that are pushing into traditional (state) security fields – it is the state that is currently trying to (re)establish its authority in a space cultivated by innovative practices of companies and consumers on the one hand and criminal actors on the other side. This is shaking up long-standing power relationships.

Expectations about the roles and responsibilities (self-assigned or with regard to other actors) are not always aligned with the expectations of others. Resulting socio-political conflicts are symptomatic for an issue that mobilises different stakeholders from different sectors with divergent interests and are an expression of the struggle over influence at the same time. Analysing the context of the different positions will help us understand both the history of cybersecurity but also what is needed for the future. Ultimately, only a careful mapping of expectations and interests will help us identify potential common ground.

THE WHY – WHY IS THIS TOPIC IMPORTANT FROM A HUMAN RIGHTS PERSPECTIVE?

Cyberspace does not belong to only one type of actor. It is a space/place in which many different stakeholders do many different things at the same time. Very often, this is unproblematic. But there are certain issues that have led to considerable tensions between stakeholders. Especially in recent years, security has become a defining driver in reshuffling tacitly accepted power-relationships.

Security means different things for different people and in cyberspace as in the real world, questions over how much security should be produced for whom and at what price are endemic to this issue. If we look at how social entities with power (mainly states and big corporations) shape the cyberdomain, including the (physical) information environment by specific security-related practices, we see how the focus on the state and 'its' security crowds out consideration for the security of the individual citizen. In other words, the type of security that is currently produced is often not security relevant to the people. That way, a problem for human security is created.

THE WHO – WHO ARE THE MAIN PLAYERS?

We will focus on three main groups of actors (but will not treat them as monolithic blocks). Input from the participants will assure that different geographical contexts are given sufficient weight.

- We focus on (different types of) states. However, we will also break up this black box to look at how different bureaucratic units within the state have sometimes quite fundamentally different ideas about roles and responsibilities (law enforcement, regulators, military, and intelligence community), which considerable impact on cybersecurity issues.

- We focus on (different elements of) the private sector. Here, we will look at different types of companies and their role. For example, there are companies who are part of the cyber-infrastructure, often companies that substantially shape the way human beings interact online. Also, there are companies not directly connected to cyberspace, but implicated by cybersecurity because they are considered as owning or operating "critical infrastructures". Both types of private sector actors assume different roles and responsibilities.

- We focus on citizens and civil society groups. We will look at how recent cybersecurity developments are impacting on our lives and we will ask ourselves who is implicated in what way by the links that exist between the international security dimensions of ICTs on the one hand, and technical, human rights, development and governance issues on the other. The How – how is this topic being addressed?

To structure the session, we will first put the state at the centre and look at its past and current relationships to the other two actor groups: the relationship between the state and the private sector on the one hand and the relationship between the state and civil society/individuals on the other. After this, we will briefly look at the relationship between the private sector and civil society.

What the state expects from the private sector and what the private sector expects from the state will be the first area we look at. On the one hand, one

of the key challenges from the view of the state arises from the privatisation and deregulation of many parts of the public sector since the 1980s and the globalisation processes of the 1990s, which have put a large part of the critical (information) infrastructure in the hands of private enterprise. This creates a situation in which market forces alone are not sufficient to provide security in most of the critical 'sectors'. At the same time, the state is incapable of providing the public good of security on its own, since an overly intrusive market intervention is a flawed and undesirable option, because the same infrastructures that the state aims to protect due to national security considerations are also the foundation of the competitiveness and prosperity of a nation.

The second area we focus on is the relationship between the state and civil society. Very often, the focus on the state and 'its' security crowds out consideration for the security of the individual citizen, not least because more security often means less freedom/liberties. In other words, the type of security that is currently produced is often not security (directly) relevant to the people. That way, a problem for human security is created, which consists of both a sustained feeling of insecurity, insecurities in the form of (material) vulnerabilities in the infosphere, and exploitation of these insecurities by several political actors.

The third area is the interesting relationship between private companies and civil society, which is the least understood of the three blocks. For example, Big Data is considered the key IT trend of the future, and companies want to use the masses of data that we produce every day to tailor their marketing strategies through personalised advertising and prediction of future consumer behaviour. What are the security implications of that? What expectations do we have?

THE WHERE AND WHEN – WHERE AND WHEN IS THE TOPIC BEING ADDRESSED?

Roles and responsibilities (both self-assigned and expected from others) are a cross-cutting issue in all cyber policy fields. Developing sensitivity to the different expectations and positions can help us understand policy processes. In addition, it will help us understand where civil society input might be warranted: Given the range of legitimacy and normative concerns as well as the technical issues involved in security matters, even deeper engagement of civil society than in other areas seems desirable.

04

CYBERSECURITY AND INTERNATIONAL PEACE AND SECURITY

VLADIMIR RADUNOVIĆ, DIPLO FOUNDATION

INTRODUCTION

States have been discussing the effects of information and telecommunications technology on international peace and security since the 1990s. Since then, several significant cyber incidents made front-page headlines and a growing number of governments have been developing new policies and institutions on the political and military use of cyberspace. As a result, an active debate is now taking place about what norms should govern behaviour in cyberspace, how to build confidence and increase stability, and how to build up the capacity of states to address cybersecurity threats within their own borders. This debate includes a number of important human rights considerations. This webinar is designed to help build understanding of the issues, the actors in play, and where and when this topic is being discussed.

THE WHAT – WHAT IS THE TOPIC ABOUT?

An increasing number of states have been integrating cybersecurity into their national security and defense strategies and some have gone so far as to implement separate defense and security strategies for cyberspace. This rise of cybersecurity from low to high politics has brought about new investment in national capacity to respond to threats and vulnerabilities and in developing cyber-offensive and defensive military capabilities. Because of heightened interest and investment at the national level, questions emerged around the applicability of traditional security concepts, laws, and governance structures to cyberspace. The discourse revolves around laws, norms, and principles that govern state action in cyberspace, confidence building measures (CBMs) for cyberspace, and capacity building measures for cyberspace.

THE WHY – WHY IS THIS TOPIC IMPORTANT FROM A HUMAN RIGHTS PERSPECTIVE?

The cybersecurity debate from the perspective of international peace and security is important for human rights proponents and humanitarians because it focuses on the norms, laws, and principles governing state actions in cyberspace. This includes, for example, discussions on how existing principles such as the

principle of distinction (the concept that militaries must differentiate between civilian and military targets), or the principle of proportionality (the concept that the destruction caused by an attack must be proportionate to the military gain achieved from that attack) apply to cyberspace. Without mature versions of these concepts and others, state action in cyberspace is potentially anarchical, and the ability of states to carry out attacks on civilians is legally and normatively untethered. Furthermore, many proposals for new laws to govern state action in cyberspace propose to codify the state's role in controlling information online. These measures pose specific threats to free expression around the world. That is why the discussion about how to define information security and cybersecurity has important human rights implications. Moreover, there are opportunities for civil society engagement on the topic of cybersecurity and international peace and security which governments have explicitly acknowledged, for example, in the context of the CBMs discussion at the Organization for Security and Co-operation in Europe (OSCE) or the UN General Assembly's First Committee.

THE HOW – HOW IS THIS TOPIC BEING ADDRESSED?

The laws, norms, and principles that govern state action in traditional conflict are grounded in a strong recognition of the value of human lives and the importance of human rights. Similar to the discussion over whether human rights apply offline as well as online and the resolution adopted by the UN Human Rights Council, there has been a debate over whether the norms codified in international humanitarian law apply offline as well as online. Some states contested that international humanitarian law applies online as well as offline until a group of governmental experts (UNGGE) from 15 countries established by the UN General Assembly's First Committee agreed that international law is applicable in a consensus report published in 2013.

Arguably the more challenging aspect of the norms discussion is how to interpret existing international law for cyberspace and what norms might have to be developed for activities that are not covered by existing law. The Tallinn Manual on the International Law Applicable to Cyber Warfare published in 2013 focus on this translation exercise. It was developed by an independent group of 15 legal experts under the auspices of NATO's Cooperative Cyber Defence Centre of Excellence. A new group is currently in the process of looking into the types of activities where there is a greater uncertainty of what type of law and norms apply.

Complementing this norms discussion is the diplomatic effort to develop CBMs for cyberspace. The OSCE adopted the first multilateral set of CBMs in December 2013. The concept of CBMs dates back to the Cold War and describes the efforts by superpowers to avoid accidental escalation or nuclear war due to misunderstandings. CBMs are designed to prevent unnecessary conflict in terms of both scale and incidence. States and other actors are now trying to develop CBMs to reduce the likelihood of conflict in cyberspace.

THE WHO, WHERE AND WHEN – WHO ARE THE MAIN PLAYERS, WHERE AND WHEN IS THE TOPIC BEING ADDRESSED?

Cybersecurity from an international peace and security perspective has been discussed in various international fora including the UN General Assembly, the G8, the London Conference process and regional organisations such as the OSCE, NATO, the Shanghai Cooperation Organization, and the Association of Southeast

Asian Nations Regional Forum.

One of the key fora is the UN General Assembly's First Committee that has been discussing developments in the field of information and telecommunications in the context of international security since 1998. This process also led to the creation of groups of governmental experts (UNGGE). A fourth group is currently in place consisting of representatives from 20 countries and expected to publish its report in the second half of 2015. It was preceded by three UNGGEs and the report published by the third UNGGE in 2013 remains the most significant because of its affirmation of existing international law, sovereignty, human rights, and governance.

In 2011, China, Russia, Tajikistan, and Uzbekistan submitted a draft version of an International Code of Conduct for Information Security, a proposal developed through the Shanghai Cooperation Organization (SCO) for new norms and laws governing state conduct in cyberspace, to the UN General Assembly. Shortly following the initial submission of the Code of Conduct, Russia also presented a draft Convention on International Information Security, which sparked debate regarding the need for a "treaty for cyberspace." In January 2015, the SCO proposed an updated draft of the Code of Conduct calling on states to prevent the use of information technologies to spread information that "incites terrorism, separatism or extremism or that inflames hatred on ethnic, racial or religious grounds." Because states define and interpret words like terrorism, separatism, and extremism in different ways, many governments and human rights experts are concerned that language like the proposed Code of Conduct would be used by states to legitimise limiting free speech and expression.

NATO has also actively discussed cybersecurity and its implications for international security. In September 2014, NATO heads of state agreed that Article 5 of the defense treaty, the collective defense clause, applies to cyber attacks as it does to conventional attacks, though they refrained from defining what kinds of attacks would invoke the clause. In addition, the Tallinn Manual on the International Law Applicable to Cyber Warfare, developed by an independent group of 15 legal experts under the auspices of NATO's Cooperative Cyber Defence Centre of Excellence, spun out of the discussions at NATO following the 2007 Distributed Denial of Service attacks targeting Estonia.

Another important forum where cybersecurity has been discussed through the lens of international peace and security is the London Process which started with the 2011 London Cybersecurity Conference. The Global Conference on Cyberspace in The Hague is the fourth conference in this series following the second conference in Budapest, Hungary, in 2012 and the third conference in Seoul, Republic of Korea, in 2013. The goal of the Global Conference on Cyberspace is "to promote practical cooperation in cyberspace, to enhance cyber capacity building, and to discuss norms for responsible behaviour in cyberspace."

SUGGESTED LITERATURE

- Kavanagh, Camino, Tim Maurer and Eneken Tikk-Ringas. Baseline Review of ICT-Related Processes and Events: Implications for International and Regional Security. 2013. Available at: http://ict4peace.org/baseline-review-of-ict-related-processes-and-events-implications-for-international-and-regional-security/

05

CYBERCRIME

DR. TATIANA TROPINA, SENIOR RESEARCHER AT THE MAX PLANCK INSTITUTE FOR FOREIGN AND INTERNATIONAL CRIMINAL LAW

INTRODUCTION

The aim of this module on cybercrime is to build awareness among civil society participants about the different approaches used to address the problem of cybercrime in a multistakeholder environment. The module will aim to explain the phenomenon of various forms of cybercrime and draw the distinction between cybercrime and national security issues in the context of cybersecurity. Furthermore, it will provide an overview of technical, legal, and organisational challenges related to fighting crime in digital networks. Finally, the training will provide an analysis of the current ways to address the multifaceted problem of cybercrime at the national and international level from different perspectives: legal frameworks (substantive criminal law and procedural law), jurisdiction, public-private collaboration, awareness raising, and capacity building.

THE WHAT – WHAT IS THE TOPIC ABOUT?

There is no commonly held definition of cybercrime. It can be referred to, in the narrow sense, only as acts against computers and information networks. However, this definition excludes many illegal activities that involve, but do not target computers and information-communication networks, such as creation, access to, and distribution of child abuse images, grooming, or identity-related crime. Yet when cybercrime is defined as any crime that involves computers or computer systems, the term becomes unnecessarily broad. Many criminal acts might possibly include the use of computers and networks; however, these activities do not constitute the substantial element of the crime, such as, for example, the use of email by drug dealers for communication.

Such important international legal instruments as the Council of Europe Cybercrime Convention, the League of Arab States Convention, and the African Union Convention on Cybersecurity do not provide a definition of cybercrime, but rather outline the acts that constitute what they call “cybercrime.” Most of them refer to crimes against confidentiality, integrity, and availability of computer data and systems; computer-related crimes such as computer fraud and forgery, illegal content; and child abuse crimes. Thus, the definition of cybercrime mostly depends on the underlying purpose behind the use of this term.

Furthermore, from the perspective of criminal justice, the term “cybercrime” should operate on a number of levels. The definition of criminal conduct should

be very specific concerning certain individual unlawful acts that entail criminal responsibility to follow the principle of legal certainty. However, for the purpose of criminal justice, the term has to be sufficiently broad to ensure that investigative powers and international cooperation mechanisms can be applied with effective safeguards and protection of privacy and human rights to the continued migration of offline crime to cyberspace. This will guarantee that digital evidence can be collected in a transparent and accountable manner within the strict legal frameworks and presented in courts.

THE WHY – WHY IS THIS TOPIC IMPORTANT FROM A HUMAN RIGHTS PERSPECTIVE?

The issue of fighting cybercrime raises several major challenges for human rights protection. First of all, there is a specific concern for the manner in which the state achieves its criminal justice goals. The law of criminal procedure and the process of cybercrime investigation should come under particular scrutiny from an international human rights perspective, because investigative measures can be simultaneously seamless and very intrusive. Furthermore, human rights standards can potentially be endangered by bulk data collection for the purpose of crime prevention. Last but not least, content-related crimes can be of particular concern. Measures taken against these crimes can restrict freedom of expression and can possibly be turned into an instrument of oppression.

THE WHO – WHO ARE THE MAIN PLAYERS?

Before the evolution of information and communications technologies, fighting crime was mostly considered to be the domain of national governments. The legal frameworks, which regulate prosecution and investigation of crime, always imply sovereignty issues and require effective mechanisms of enforcement, which are based on hierarchical structures and command-and-control approach. The decentralised architecture of the internet is eroding old paradigms of the division of responsibilities between government, the private sector, and civil society even in less flexible areas such as criminal law and criminal investigation. The problem of cybercrime requires the development of effective solutions at various levels, both national and international, and involves both non-governmental and governmental stakeholders.

Thus, industry intermediaries (not only ISPs) are becoming “critical nodes” for preventing and investigating cybercrime and safeguarding the security of their customers. While national governments have the power to establish and enforce legal and regulatory frameworks, the private sector, which owns and manages the ICT networks and offers the services, better understands the changing and converging nature of the ICT environment and has greater adaptability towards new technologies, more expertise, and resources to produce an adequate response to cybercrime threats. Involvement of the private sector in fighting cybercrime is being developed at the national level in many countries far beyond ad hoc collaboration for investigating particular cases of cybercrime or blocking and removing illegal content. It is taking the form of industry cybercrime codes of conduct, public-private reporting platforms, multi-industry public-private collaboration programmes against cybercrime, national botnet detection and mitigation projects involving internet service providers, to name but a few.

Civil society has always been considered an important stakeholder for raising awareness about cybercrime and helping citizens to understand that each person is a crucial part of a larger 'security chain.' However, one of the most prominent roles of civil society is ensuring transparency, safeguards, and human rights protection concerning cybercrime prevention and investigation. This is because electronic communications enable bulk data collection and the accompanying investigative measures can be simultaneously seamless and very invasive.

Since the trans-border character of cybercrime calls for counteractions that are coordinated on different levels – national, regional, and global –international and regional organisations, both governmental and nongovernmental, are also important stakeholders. They deal with a range of issues from harmonisation of substantive criminal and procedural frameworks, (E.g. The Council of Europe) to operational coordination of cybercrime investigations (E.g. Europol), capacity building, awareness raising, and human rights protection.

THE HOW – HOW IS THIS TOPIC BEING ADDRESSED?

The problem of fighting cybercrime reflects the tension between nonflexible legal frameworks – which, like criminal law, were not meant to be flexible by their nature – and the non-hierarchical structure and borderless nature of the information and communications networks that do not fit the traditional top-down command and control models. Until quite recently, the problem of cybercrime was considered mainly a legal issue that focused on updating old legal frameworks, which were not applicable to the crimes committed in cyberspace, and development of procedural measures to address the new technologies and trans-border component of the problem.

However, today cybercrime is not considered solely a legal matter. Though law (especially compatible substantive legal frameworks to avoid safe havens for cybercriminals) is one of the most important components of tackling the illegal use of information networks, criminal law can only react to the problem when a crime has already taken place. Proactive measures, in addition to reactive approaches, include capacity building and collaboration among the public sector, private companies, and civil society to provide training and education, to raise awareness about cybercrime, and to make cyberspace a safer place for businesses and users.

THE WHERE AND WHEN – WHERE AND WHEN IS THE TOPIC BEING ADDRESSED?

Crime in the digital environment is a fast-changing multifaceted problem; addressing it is always like chasing a moving target. There is no 'one fits all' solution as well as no legal and policy frameworks that can cover every aspect of the problem and solve it in the short term. Understanding the complexity of the ecosystem, a combination of using a top-down approach for criminal law enforcement and a bottom-up approach, along with collaboration between public and private stakeholders, transparency, and accountability, are the necessary components of any strategy to tackle cybercrime.

Since the problem is transborder, there are two levels at which to address it: national and international. In the field of harmonisation of legislation, binding and nonbinding international legal frameworks related to cybercrime were created by the Council of Europe, the European Union, the Commonwealth of Independent

States, intergovernmental African organisations like the African Union, and the League of Arab States. However, the issue of tackling cybercrime has been on the agenda of different international organisations and agencies. The G8 Group of States, Organisetion of American States (OAS), Asia Pacific Economic Cooperation (APEC), The Organisation for Economic Co-operation and Development (OECD), Association of South East Asian Nations (ASEAN), Interpol and Europol, and many other organisations are dealing with cybercrime policy and strategy, the harmonisation of legal frameworks and operational activities, capacity building, and awareness raising. On the national level, there are many forms of addressing the problem of crime in digital networks: adoption of legal frameworks to investigate and prosecute cybercrime, awareness raising campaigns, training and capacity building, prevention, detection, and early disruption. The involvement of the private industry and civil society can be witnessed on both the national and international level concerning all forms of fighting cybercrime. Many countries and international organisations are trying to get industry and civil society organisations engaged in policymaking and lawmaking processes in a top-down manner, via stakeholder consultations to ensure transparency and protection of privacy and human rights. However, the bottom up approaches and voluntary initiatives of private industry actors and civil society activists are also very important components of fighting cybercrime on the national level.

SUGGESTED LITERATURE

- UNODC. *Comprehensive Study on Cybercrime*. 2013. Available at: https://www.unodc.org/documents/organized-crime/UNODC_CCPCJ_EG.4_2013/CYBERCRIME_STUDY_210213.pdf
- Rob van den Hoven van Genderen. *Cybercrime investigation and the protection of personal data and privacy. Discussion paper.* 2008. Available at: http://www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/Documents/Reports-Presentations/567%20study5-d-provisional.pdf

06

CAPACITY BUILDING

VLADIMIR RADUNOVIĆ, DIPLO FOUNDATION;
TAYLOR ROBERTS, GLOBAL CYBER SECURITY CAPACITY CENTRE, UNIVERSITY OF OXFORD

INTRODUCTION

Cybersecurity capacity building has become an area of common interest for several governments across the world. However, there is little common understanding as to what capacity in cybersecurity consists of. This training will provide participants with a fundamental understanding and overview of the landscape of cybersecurity capacity building.

THE WHAT – WHAT IS THE TOPIC ABOUT?

The webinar and training will focus on cybersecurity capacity building with a focus on freedom, security and growth. Cybersecurity capacity should not be limited to technical capacity, but expanded to include policy and strategy, society and culture, education and training, legislation and regulation, as well as standardisation and market development. Capacity building goes far beyond single training - it needs to be approached comprehensively and with a blended-learning format that should ensure learning and understanding, allow time for reflections and building own positions, then coaching people into getting involved with policy processes and being comfortable to engage and contribute within them.

THE WHY – WHY IS THIS TOPIC IMPORTANT?

Capacity development has been a central theme within development for several decades. In order to ensure that people around the world can reap the benefits of the Internet and information communication technologies (ICT's), capacity building in cyberspace has now become a pillar of many government's foreign policy approach, and has emerged as a potential area of cooperation not only between governments, but also between public, private and civil society sectors.

Given the breadth of cyber capacity building fora, there are several areas of potential benefit as well. Building policy for development in cyberspace will enhance the overall strategic coordination and implementation of efforts. Raising awareness of cybersecurity and other initiatives will increase social participation in key debates, ensuring societal values are taken in consideration when developing policy and legislation, while at the same time raising the overall

security and economic level of the country. Formal education and training in ICT and cybersecurity will enable social growth through a more technically skilled workforce. Building frameworks for legislation and regulation on issues concerning cyberspace will help to ensure freedoms, security and economic growth. Finally, implementing technical standards will enable the adoption of best practices during technical infrastructure development.

THE WHO, WHERE AND WHEN – WHO ARE THE MAIN PLAYERS, WHERE AND WHEN IS THE TOPIC BEING ADDRESSED?

Capacity building is necessarily a multi-stakeholder endeavor, as cyber capacity spans the public, private and civil society sectors. Here is a non-exhaustive list of actors that may be involved:

- ministries
- information technologies
- defense
- interior
- foreign affairs
- education
- health
- economy
- commerce
- transportation
- justice and attorney general's office
- academia
- Internet governance representatives
- Internet Society chapters
- criminal justice community
- intelligence community
- legislators
- national security representatives
- CERT/CSIRT teams
- major commercial sectors and SME's
- finance sector
- telecommunications companies.

An approach which involves different stakeholders and professional cultures enables knowledge-sharing across these institutional silos, and improves inter-professional communication and understanding. It also enables a more holistic understanding of cyber-security, discussed from various angles: technology, law, economy, societal perspective, international relations and diplomacy.

Regardless of whether a new capacity building program is being developed, or if an institution is looking for partners to implement an existing one, there are several dimensions to look at, depending on the target audience:

- For Whom: The capacity building program needs to be adjusted according to specific target audiences. Thus the main starting question is who is the target audience (e.g. technical community, law enforcement, governmental institutions, corporate sector, youth activists)? Besides, what is the target level of the targeted audiences (high level, coordination and management level, operational level)?

- What: What is the thematic focus (e.g. overall cybersecurity, cybercrime, international peace and security, Internet safety and child protection, digital rights, policy and strategic planning, Internet governance)? What is the desired perspective (e.g. policy, technology, legal, diplomatic)?

- Where and when: Traditional approaches include in-situ workshops, panels, simulations, case studies etc. The Internet has also enabled online courses, webinars and similar 'remote' events enabling remote participation at lower costs and extending the outreach from national to regional or global level participation. Timing is equally important and the combination of online and in-situ activities throughout the year(s).

THE HOW – HOW IS THIS TOPIC BEING ADDRESSED?

There are several organisations with various areas of expertise that seek to enhance cyber capacity building. Some organisations, such as the Forum for Incident Response and Security Teams (FIRST) and the International Telecommunications Union (ITU) have invested resources in Computer Incident Response Team (CIRT) development. Other organisations, such as the European Union Agency for Network and Information Security (ENISA) and Organisation of American States (OAS) have adopted a regional approach to capacity building, working with particular countries across a range of capacity building areas, such as national cybersecurity strategies and crisis management. Given the breadth of cybersecurity issues, the Global Cyber Security Capacity Centre at the University of Oxford has developed a capability maturity model (CMM) that helps a nation comprehensively assess their cybersecurity capacity in order to guide more strategic investment. In addition to these organisational approaches to capacity building, individual countries have begun to develop programmes that seek to deliver capacity in various areas.

In order to connect these numerous initiatives together, GCCS 2015 will launch the Global Forum on Cyber Expertise, which seeks to stimulate new funding streams and the sharing of expertise and experiences. By matching supply and demand, countries that lack knowledge in certain cyber areas can benefit from the knowledge and expertise that will be provided by countries and companies with more experience in cyber matters.

CONCLUSION

Capacity building has become a very frequent term in cybersecurity-related discussions around the globe. At the same time, developing an effective and efficient capacity building program is not easy - it requires sustainable funding, skills, continuity and comprehensive methodology and didactics. In developing new programmes or engaging with the existing programmes, it is important to look into specific elements that can ensure the desired impact. There is number of existing capacity building programmes around the world, which should be better mapped and utilised.

SUGGESTED LITERATURE

- Global Cyber Security Capacity Centre, Cyber Security Capability Maturity Model, https://www.sbs.ox.ac.uk/cybersecurity-capacity/explore/home?type=model
- DiploFoundation, About Diplo's capacity development, http://www.diplomacy.edu/capacity/more
- LENCD, SDC, UNDP, Learn4Dev and DiploFoundation, Capacity Development, http://www.diplomacy.edu/courses/capacity

07

PRIVACY

ANDREW PUDDEPHATT, GLOBAL PARTNERS DIGITAL

INTRODUCTION

The purpose of this webinar is to discuss the meaning of privacy in a cybersecurity and human rights frame, exploring how the notion of privacy and its realisation is changed by the Internet, technically, commercially and normatively. We will identify the range of factors shaping the way that privacy is being affected online and the roles and responsibilities of different stakeholders.

THE WHAT – WHAT IS THE TOPIC ABOUT?

Privacy has different meanings in different contexts and societies. At its heart is the idea of the security and integrity of a human being and their control of their immediate environment and what is known or can be known about them.

Exact definitions of privacy are elusive – national and international courts have refused to provide clear definitions of privacy. At a general level privacy is understood to be protection from "arbitrary or unlawful interference with his privacy, family, home or correspondence, … [and] unlawful attacks on his honour and reputation." Thus protection of reputation (from defamation) is linked to privacy which creates tensions between freedom of expression rights and privacy rights. Anonymity and encryption, sometimes referred to as rights by activists, should be more properly regarded as enablers of rights – both of privacy and free expression.

It should be noted that privacy is not the same as data protection. Data protection policy has rules designed to address the systematic collection of data about individuals and the policies applying to all personally identifying data held by designated 'data controllers'. Privacy, however, is more fluid concept applying to information about which a person may have a reasonable expectation of privacy.

Throughout history the understanding of privacy has changed depending upon societal and technical developments. While the notion of personal integrity and dignity lies at the heart of privacy as it does of all human rights, it has a different meaning in a communal village to that of a modern city. Two big factors affecting the way we understand privacy are the emergence of generalised private property (single households) and communications technology. For example the modern understanding and debate about privacy grew from debate about publishing photographs of people in newspapers at the end of the nineteenth century. There is therefore no exact boundary to the definition of privacy, and a dramatic

technological change like the Internet will inevitably re-shape understandings of privacy. This may help explain the contrast between what people say about privacy and the internet and how they behave.

THE WHY – WHY IS THIS TOPIC IMPORTANT FROM A HUMAN RIGHTS PERSPECTIVE?

Technically the internet enables the collection of new types of personal information; facilitates (and economically demands) the collection and location of personal information; creates new capacities for government and private actors to access and analyse personal information; creates new opportunities for commercial use of personal data and sets new challenges for regulation given the transnational nature of the internet.

In addition new internet services redefine the privacy environment dramatically - cloud computing (raises questions of security, data breaches and ownership); search engines (systematically tracking and monitoring our behaviour); social networks (depend on a company led exchange and analysis of data provided by users); the mobile internet ties internet use to geo-located devices; and the Internet of Things connecting all potential objects which together convey a complete picture of our lives.

And governments are increasingly relying on digital platforms to provide services through use of data with designated e-identities that allow services, banking, voting, health monitoring etc. The sheer volumes of data available privately and publically make it difficult to conceive that governments won't seek to access it.

Moreover governments have become increasingly concerned about security issues online – for both legitimate and illegitimate reasons. All governments are attempting to access information online to the limit of their technical ability, raising serious concerns about:

- Scope of surveillance (who are the targets and how big is the net)
- Legal framework of surveillance
- Use of mass metadata searches excluded from legal accountability
- Weakness of oversight
- Absence of legislative competence
- The provision of many internet services based on a business model based on advertising.

We trade or cede our privacy in exchange for free services. Such service models either directly depend upon exposing private information (Facebook), or they intrude on privacy to create efficiencies (e.g. tools that optimise searches based on tracking user preferences). Generally there is little real public pressure or incentives to challenge this model and informed consent to data use for users online is complicated by range of different applications, complexity of terms of use, and apparent public indifference.

So the key question is: how to protect privacy and individual liberties while enabling the free flows of personal data and maintaining security of personal data. This will depend upon strong security both technically – encryption – and normatively – with appropriate legal rules governing access to and use of personal information.

THE WHO – WHO ARE THE MAIN PLAYERS?

There are two areas to focus on -

- The implications of developments in private sector and where the technologies and markets are leading.
- The use of personal data by governments – not just security surveillance but wider recasting of citizen/government relationship digitally – tax, health, etc.

At the heart of the notion of privacy lies sense of personal integrity and dignity whatever the social context. At the core of this is sense of ownership and control, i.e. consent to use of information (basis of data protection system) and what can be known. Current business models require us to hand over ownership of our data to companies in exchange for benefits -use of that data is loosely regulated if at all. How do we control this?

Companies should practice greater transparency about data management practices, provide accessible and reasonable terms of service, explore shift of business model to one where there is greater user control of data with the ability for users to own data and grant permissions for use and encourage higher standards of encryption and anonymity, as both are enablers of privacy rights and publish details about government requests for user data.

Governments should commit to ensuring user security and privacy as a policy goal, commit to freedom of expression (aware of the need to balance both rights), understand cybersecurity as embracing users interests, be transparent about the rationale and scope of surveillance or other measures violating privacy and ensure that rules governing surveillance and privacy violations are grounded in law, consistent with international principles and subject to supervision by independent courts and finally regulate effectively e.g. by having technical skills on regulatory bodies.

Lastly civil society has an important role to represent user rights and consumer interests, to bring concerns from excluded and marginalised groups, to provide innovative ideas and policy options; to champion a human rights and public interest approach to privacy policy.

THE WHERE – WHERE IS THIS TOPIC BEING ADDRESSED?

Ten years ago, the International Law Commission concluded that "no homogenous hierarchical meta-system is realistically available" within the international legal order to resolve detailed differences among the separate spheres, that this would have to be left to the realm of practice. This means little prospect of a global privacy policy – so how can it be 'practiced'?

Among the important venues for policy are:

- **Policy forums** - International Conference of Data Protection and Privacy Commissioners discussions, Internet Governance Forum
- **UN normative standards setting** such as the UNGA (resolutions on privacy),
- Recommendations such as the OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data
- **UN Special procedures** e.g. UN Human Rights Commissioner (recent report on privacy); new Special Rapporteur

- **Technical bodies** – e.g. Internet Engineering Task Force (IETF) - work on increased encryption standards, RFC 6973, RFC 6772, RFC 6280
- **Regional courts** – ECHR generic privacy cases and **national courts** – Yahoo, Louis Feraud judgements.

GLOBAL PARTNERS DIGITAL

Development House
56–64 Leonard Street
London EC2A 4LT

+44 (0)20 7549 0336

gp-digital.org