SECURITY IN TRANSITION:
AN INTERDISCIPLINARY
INVESTIGATION INTO THE
SECURITY GAP

Cybersecurity: a case for a European approach

Emmanuel Darmois and Geneviève Schméder

Paper commissioned by the Human Security Study Group

FRIEDRICH EBERT STIFTUNG

SiT/WP/11/16

erc

LSE International Development

Emmanuel Darmois is a French specialist of Information and Communication Technologies. He started his career by teaching Computer Science and working on Artificial Intelligence. He has since occupied a variety of positions in the industry, in research, technical strategy and development, or standardization. He is currently involved in projects with the European Commission on Cloud Computing and Internet of Things.

Geneviève Schméder is a French University Professor who taught in Science Po and various universities in France and elsewhere. She previously worked in the OECD and in the French Ministry of Industry and was an early member of the Human Security Study Group which reported to Javier Solana, EU High Representative.

Contact

Emmanuel Darmois: emmanuel.darmois@commledge.com
Geneviève Schméder; gschmeder@wanadoo.fr

Security in Transition
February 2016, London

Abstract

Everyday civilian and military activities have become highly dependent on cyberspace. This creates new vulnerabilities both to accidents and to intentional threats. Malevolent individuals and organisations may, without any physical presence, infiltrate all possible networks, including the most sensitive ones. Every individual as well as governmental, non-governmental and business organisation may be targeted. Hence the growing concern for cybersecurity, which reflects the changes taking place in broader approaches to security - from the security of nations and territories to the security of individuals and communities. As cyber threats transcend international boundaries, concern mostly civil societies, and are in essence asymmetrical and have a crucial human rights dimension, they relate to human security rather than to traditional security approaches. After some examination of the content and the actors of cybersecurity and the links to human security, the paper focuses on EU policies in this field and their specificities. It ends by identifying a distinctive EU approach to cybersecurity, which rejects the kind of technological determinism and mass surveillance that characterise the approaches of other key actors.

Table of Contents

Introduction

Everyday operations of business, government and civil society have become inseparable from activities in cyberspace. This digitalisation of our societies offers huge benefits, but it also creates new vulnerabilities both to accidents and to intentional threats. Malevolent individuals and organisations may, without any physical presence, infiltrate all possible networks, including most of the sensitive ones; and modify the behaviour of applications and compromise data. Every individual as well as every governmental, non-governmental and business organisation may be targeted.

Hence the growing concern for cybersecurity, which matches the changes taking place in the approach of security -from the security of nations and territories to the security of individuals and communities. Even though the notion of cybersecurity is deeply and increasingly embedded in contemporary military practices, cyber threats have several characteristics that relate them to human security rather than to traditional security approaches: they transcend international boundaries, mostly concern civil societies, and are in essence asymmetrical and have a crucial human rights dimension.

This paper deals with some of these issues. After some clarifications on the content and the actors of cybersecurity and how it relates to human security, it will focus on EU policies in the field and their specificities. It ends up in shaping a distinctive EU approach to cybersecurity that does reject the kind of technological determinism and mass surveillance that tends to characterise the American approach.

I Cybersecurity: nature and reality of threats

Though there is no widely accepted definition of cybersecurity, the USA National Institute of Standards and Technology (NIST) provides a condensed one[1]: "The ability to protect or defend the use of cyberspace from cyber attacks". It has the merit of directly pointing to two key aspects: the very large span of the problem domain – reduced in scope for the purpose of the present paper - and the central role of aggressive behaviours – where some reality check may prove useful.

[1] The NIST security glossary: http://nvlpubs.nist.gov/nistpubs/ir/2013/NIST.IR.7298r2.pdf

Motivations and attacks

In a broad sense, cybersecurity has to do with the prevention, detection, mitigation and response to destructive or malevolent practices developed in cyberspace that affect computer systems and their associated data. To better characterise these practices, it is probably useful to distinguish their motivations from the methods and technologies used to undertake them.

Regarding the intentions of the attackers, they are extremely varied and range from the least damaging to the potentially catastrophic. Some examples of these intentions are listed below by growing order of negative impacts:

- Recreation and narcissism: e.g. pride and glory of being an intruder, fun of propagating jokes, hoaxes, scams, etc. Though these attacks are often directed to individuals, they are generally considered as out of the cybersecurity scope.
- Activism: e.g. support of civil society in difficult political environments, whistleblowing, and actions against other groups perceived as threats. Though activism is very often considered as illegitimate by existing powers, the supporting actors – and hence the civil society – may need to be protected. In some cases, the actions of activists fall in the next category.
- Disinformation and vandalism: e.g. dissemination of false information, corruption of web sites and data, blockade of information channels[2]… Though making use of spamming, viruses and malware[3], this kind of attacks usually disrupt nonessential services or are mainly a (costly) nuisance. They may induce the disruption of the target but are not always undertaken with this as a primary goal.
- Economic interest and greed: e.g. sexual abuse (in particular children abuse); money extortion and laundering, illegal trade, sale and purchase of stolen data. All are a very fast growing segment of cyber criminality.
- Espionage and interceptions, theft of sensitive data (personal data, intellectual property, R&D, business-strategic data, etc.). All states and many companies are victims of cyber espionage activities, many of which are sponsored by states.
- Sabotage: e.g. attacks against the (physical or informational) integrity of critical infrastructures that are used in the production or the provision of crucial goods and services, provided by governments or the private sector, and which are crucial to citizens' lives (energy, transportation, water, communications, etc.). In the extreme case, the intention may be to cause bloodshed through accidents or disasters.

[2] Newspapers are privileged targets of cyberterrorists.
[3] http://arstechnica.com/security/2015/04/botnet-that-enslaved-770000-pcs-worldwide-comes-crashing-down/ (25/11/2015)

The gradual creation of the cyberspace since the end of the 70's has generated a number of "enabling factors":

- Anonymity. The Internet environment - intended as the network of all networks, including the mobile ones - affords perpetrators the ability to disguise themselves under the cover of involuntary relays or intermediaries.[4] Seizing control of intermediary systems to launch an attack prevents tracing, so that targets are not certain of the source or who is behind it.

- Impunity. Malicious attacks do not require geographic proximity to their target and thus present a low risk for attackers. They can avoid being discovered and prosecuted by covering traces and exploit the gaps and loopholes of legislations.

- Flexibility. Technology offers a variety of options regarding the nature of attacks. Direct attack is in general the most effective, but may be risky with respect to anonymity, and may suggest indirect means. This is the rationale behind the perpetration of attacks like the Distributed Denial of Service (DDoS), which saturates the operation of a network by using slave computers to send millions of requests that cannot be handled, and makes the service unavailable.

- Reduced investment. Cyberspace affords strong leverage with low investment since attacks can be cheap (many tools are downloadable for free) and relatively easy to organise with limited resources, basic skills and mainstream computers.

But the main factor for the development of cyber threats is the proliferation of vulnerabilities. Today's cyber systems have complex architectures (e.g. systems of systems), are highly interdependent and hard to test exhaustively, and require vulnerable end-user devices (e.g. smartphones). On top of the technical defects, the “human factor” (people who, either by lack of attention or by ignorance, are a weak link) creates other vulnerabilities: in classified military networks, for instance, nearly all penetrations and breaches occurred because of this. [5]

The reality of threats

Amongst the classes of attacks cited above, most have become mainstream, extremely frequent and have growing negative economic, societal and security consequences.

In the business world, in particular, companies and legal actors are in a difficult defensive position. As most cyber attacks are not very sophisticated, many companies tend to underestimate the risk, though it may be lethal (theft of digital capital, divulgation of

[4] A frequent method is known as the “man-in-the-middle” attack, i.e an attack where “a third party attacker inserts himself between two participants in a conversation and automatically relays messages between them, without either participants realizing it. This third party acts like an invisible intermediary, having tricked each participant into believing that the attacker is actually the other party of the conversation” (Eric Schmidt and Jared Cohen, *The New Digital Age: Reshaping the Future of Peoples, Nations and Business (2013)*

[5] One of the most striking was the hacking of the personal AOL email account of the head of CIA.

confidential data from banks, dating sites, etc.). In addition, actors under attack are generally reluctant to communicate on their problems, for fear of loss of reputation or of negative reactions of customers or stakeholders. Furthermore, effective cybersecurity requires huge investments, and securing just a link in the chain is not enough. Economic actors thus have to make arbitration, for instance between cybersecurity and R&D. Yet, it seems that the cost of poor cybersecurity is still considered as bearable and that arbitration against cybersecurity spending persists.

Things may change now with the emergence of "sabotage" as a new frontier for cyber criminality. Though, so far, deadly incidents have not occurred, the worst may be still to come, in particular with the emergence of Intelligent Transport Systems, eHealth, Smart Grids or the Internet of Things. Indeed, technically, it is already feasible and possible (or it will be soon) to get control of some connected objects, including autonomous vehicles (cars, planes, possibly trains), or to disrupt elements of electricity distribution networks, water treatment plants, emergency services, and so forth. Whether this is going to happen will depend on a variety of factors, amongst which, fortunately, the capacity of cybersecurity to offer valuable and acceptable countermeasures.

II Actors, cybercrime industry and the role of governance

The cyberspace battlefield is often represented –especially in movies– as a fight between "attackers" and "defenders". The emphasis put on rogue individuals does not take into account two important aspects of cybersecurity: cybercrime as an industry, and the role of transparency and governance.

Cybercrime as an industry

The proliferation of vulnerabilities has created a number of opportunities for organised criminality. To address this very complex new market, cybercrime has developed innovative approaches to foster skills specialisation and the associated creation of "value-chains" and "ecosystems", like in the legal high-tech industry.

A flurry of new and specialized "small jobs" has surfaced to exploit vulnerabilities [6]. This division of labour has allowed sharing the risks, but more importantly reducing the amount of knowledge needed. Cyber criminality is systematically keeping busy with new and advanced techniques, even if individual cybercriminals aren't. As a result, the speed with which tools and techniques used to perform cyber attacks continuously accelerates, and the sophistication of attacks is permanently outstripping the sophistication of organizations' defences. Year after year, the frequency and the severity of cyber attacks increase and countermeasures become more complex and require greater investments.

[6] http://ccm.net/contents/40-assessment-security-and-types-of-hackers

The contrasted roles of state actors

Cyber threats come from different types of actors with a variety of motivations: nation-states, cyber vandals, criminal syndicates, intruders hired by unscrupulous competitors, disgruntled insiders, etc. Amongst them, states have an eminent role and can be (and very often are) involved in a wide range of actions, from disinformation, vandalism, economic cyber criminality, espionage, to - possibly - sabotage. Despite different approaches, they all use their cyber capacities to pursue their military, economical and political objectives. Most of them are mobilizing important resources and have cybersecurity activities which are both military and civilian, defensive and offensive. As they are patient, persistent and have considerable resources, they are behind the most sophisticated cyber threats.

In the military field, there is a general claim that "action in cyberspace is part of the future battlefield"[7] and thus most governments develop capabilities to back traditional military operations by digital strikes intended to sabotage the enemy's equipment, infrastructures, communications and operations. In addition, some consider that offensive defence is not enough and they include pre-emptive cyber attacks in their global panoply. A number of states - notably the US, Russia and China, but also Iran, Israel and several European countries - are equipped for aggressive cyber-war, that includes computer network attacks, conducting damaging industrial espionage, and theft of economically significant intellectual property.[8] The major stakeholders in that field, which is largely shrouded with secrecy and over-classification, are national defence and intelligence agencies.

In the economic domain, all governments consider as their minimum obligation to have capabilities to defend their domestic infrastructures, economy and other assets, even in times of peace. This eventually includes developing deterrence through credible counter-strike capability. This defensive approach is well in line with the protection role that can be expected from the nation-state but, in concrete day-to-day operations, it is more fulfilled by the private sector itself, and the support from state agencies remains minimal.

When it comes to the political dimension, the situation is different. Quite visibly, states are using their cyber capabilities to push their political agendas against civil societies, very often starting with their own one. Though it is extremely easy to find examples of such behaviour, it is very difficult to find nation-states which have a genuine policy of using their cyber capabilities to defend their civil society. From this standpoint, the case of the USA - and the role of the United States National Security Agency's (NSA) - is very typical. The recent evolution in France after the Paris terrorist attacks is another example of trading protection against terrorists for a restriction of civil rights.

---

[7] Nick Harvey, British Minister of Defence, http://www.theguardian.com/commentisfree/2011/may/30/forget-cyber-maginot-line (10/31/2012)

[8] Richard Clarke, Cyber War, 2010 "Cyber War"

It is generally agreed that there will be a "before and after Snowden": these revelations brought to light the magnitude of US covert illegal operations in the cyberspace and raised a public debate worldwide over the legality of US governmental compliance with democratic principles. What is less visible is that there is a "before and after NSA": for a number of years, the NSA has developed an incredible amount of very sophisticated technologies directly targeted against individuals (communication interception, data theft, etc.). The life of active participants in civil society has thus become increasingly difficult, due to the existence of this set of counter technologies and to the governments' pressure – generally justified in the name of the fight against terrorism - against the use by the public of protective technologies such as encryption.

Cybercriminals and terrorists

Non-state organisations that are in the role of villains include hackers, organised transnational criminals and, increasingly, terrorist and jihadist networks and organisations. Cybercriminals with a financial motivation have become a new and dangerous breed of hackers using cyberspace for their traditional activities. They attach a great price to discretion and have a strong incentive to permanent innovation, using state-of-the-art techniques (e.g. encryption, address concealment, data anonymisation, and digital transactions). As a result, the capacities of cybercriminals now rival those of developed nations.

This parity of skills and the need for some military and intelligence services to hide their aggressive and malicious actions, hiding behind or manipulating other actors, make it useful for some nation-states to support cyber "ecosystems" that can perform legal and illegal operations. Beyond the potentially lower costs, the main advantage of leaving the attacks to informal cyber-gangs - rather than trying to organize a formal cyber-army is that states can deny responsibility for the attacks. An example of such ecosystem was the “spontaneous”, bottom-up mobilization of volunteer cyber-attacks observed in 2008 during the conflict between Russia and the Republic of Georgia.[9]

Terrorists and jihadist organizations have also soon recognized the benefits of using the Internet as a part of their technical and political arsenal. Since September 11th 2001, there is a proliferation of jihadist forums routinely used to communicate, raise funds and finance criminal activities, provide guidance to apprentices, distribute messages and PR material (e.g. beheadings and executions), and eventually coordinate physical attacks. Authors of the January 2015 terrorist attacks in Paris, for instance, were instructed on Internet from abroad.[10]

[9] According to The Economist, Russian nationalists who wished to take part in the attack on Georgia could do so from anywhere with an Internet connection, simply by visiting one of the several pro-Russia websites and downloading the software and instructions needed to perform a Distributed Denial of Service attack. Interestingly, as Russian officials underlined, NATO and the experts of the European Commission could never prove the official participation of the Russian government.

[10] The sender, likely based in Syria, used a fake account sent through a web mail based in the US. No words were used in the message that could trigger the watchdogs of intelligence services.

So far, however, despite scenarios in which sophisticated cyber-terrorists break into critical infrastructures, no single instance of real cyber-terrorism has been recorded. Terrorist cyber-attacks have become numerous, but they have not inflicted the kind of damage that would qualify them as cyberterrorism (violence against persons or property leading to death or bodily injury, or provoking severe economic loss).[11]

Yet, as a new, more computer-savvy generation of terrorists comes of age, the danger seems set to increase. Success in the "war on terror", paradoxically, is likely to make them turn increasingly to unconventional weapons such as cyberterrorism. They are aware that transition from terrestrial to virtual attacks would upgrade their nuisance capacity, [12] particularly in terms of psychological impact, media appeal and potential to inflict massive damage.

Transparency and governance

Though their most active enemies in cyberspace are nation-states (and their potential hacker allies), civil societies are not defenceless. To a large extent, their best support in cyberspace is certainly coming from a certain form of consensus – at least in democratic countries - on their legitimate right to organize, to use appropriate technologies (even if they are also used by various villains), and to promote an "open" organization and governance of cyberspace, as illustrated below.

When it comes to the support of technology to the organization and protection of civil society in cyberspace, the minimum requirements are: protection of identities (e.g. masking their real IP network address), and protection of content of communications (e.g. using encryption). In most countries, governments and government agencies systematically attempt to delegitimise the right to use those technologies, supposedly because this would undermine the state's security capabilities. For instance, some officials in the French Ministry of Interior have proposed, after the November attacks in Paris, to ban the usage of the TOR network in France (something Iran and China have tried), causing a surge of negative reactions from the civil society and forcing the French PM to officially announce this was not an option. This is surely not the last attempt.

The efficiency of civil societies in cyberspace is largely relying on the existence of the Internet, and more specifically on its "openness" which rely on a few pillars. The first one is the possibility to deploy new applications and services in a very simple – and almost not controlled – way: for instance, it is possible, with very few resources, to set up a dedicated social network. The second one is the availability of a vast number of cheap or free resources (e.g. devices, software tools, etc.) that can be easily assembled and set-up.

[11] Gabriel Weimann, Cyberterrorism How Real Is the Threat? Institute of Peace. http://www.usip.org/sites/default/files/sr119.pdf

[12] http://warontherocks.com/2015/09/is-the-islamic-state-a-cyber-threat (2015/11/14)

A third and less well-known pillar is the "open" and transparent governance of Internet. A typical example of the issue at stake is ICANN (Internet Corporation for Assigned Names and Numbers), the US-based non-profit organization that is in charge of the methodology and maintenance for the databases of identifiers and names in the Internet. Since years, there is a gradual evolution of ICANN from a US official agency towards a more transparent organisation, in the hope of ensuring that no single country has the control of this essential part of the Internet architecture. A scenario is under debate to transform ICANN into a UNO agency (under the umbrella of the International Telecommunications Union). While partisans of a lesser USA-centric governance welcome in principle this scenario as an example of multi-stakeholder governance, its most active supporters are the nations that expect they will be able to gain control on the ICANN databases for their countries, and exert a strict control on the IP addresses (thus making the life of the opponents more difficult). Probably, the least damaging solution for the civil societies is somewhere in between, with an appropriate form of governance.

The very fragile balance between civil rights and security is constantly put in question by the governments (and also quite often by the media) under various pretexts, the most prominent at the moment being the fight against terrorism. Obviously, nation-states feel entitled to support a defensive and offensive approach in their military or economic cyber strategies but, when it comes to civil societies, governments hardly feel the urge to defend them, quite often the opposite. From this standpoint, the EU is developing a different approach that is addressed in the next sections.

III The EU's approach to cybersecurity

Cybersecurity has been a preoccupation for the EU for many decades. Yet until recently, there was no coherent and coordinated EU policy in that field and some key dimensions -in particular cyberdefence-, were missing. On the one hand, Member States considered that cybersecurity was predominantly their task and prerogative and they were reluctant to adopt a common EU approach. On the other hand, the subsidiarity principle applied, because of the cross-border nature of information systems (any significant disruption in one Member State may affect other Member States and the Union as a whole), and of the potential impact of concerted policy actions on the effective protection of fundamental rights, personal data and privacy.

European initiatives in the domain of cybersecurity were initially elaborated in an ad hoc and fragmented manner and dispersed across many institutions, regulations and directives. In 2002, the Council of Europe had a pioneer role when it wrote out the Convention on Cybercrime, also known as the *Budapest Convention*, the first (and still unique) binding international treaty to address crime committed via computer

networks.[13] Entered into force in 2004, the Convention embodies a commitment and provides an effective framework to harmonise national cybersecurity legislation.

The first EU actions in cyberspace were to fight cybercrime and protect critical information infrastructure. The EU then progressively addressed the whole spectrum of cybersecurity, from law enforcement to the "Digital Agenda", and to defence, security and foreign policy.

The main objective of the Digital Agenda for Europe, adopted in May 2010, was to promote information technologies for economic and social purposes. As regards cybersecurity, it called on the Commission to establishing a permanent Computer Emergency Response Team (CERT) for EU institutions, and on Member States to establish their own CERTs, paving the way to a EU-wide network. In Sept. 2012, the CERT-EU was created. It was composed of IT security experts from various EU bodies. Besides operating for the 65 EU institutions and agencies, the CERT-EU cooperates closely with CERTs in the Member States and beyond. It also works with specialised IT security companies in order to rapidly and efficiently react to information security incidents and cyber threats on a 24x7 basis.

The European Cybersecurity Strategy

Presented in February 2013 by the EU Commission and the EU High Representative, the European Cybersecurity Strategy was the first attempt to set the stage for an overarching approach to cybersecurity in the EU. It includes and coordinates policies across formerly separate areas, in particular civil aspects of cybersecurity and cyber defence for the Common Security and Defence Policy (CSDP).

The Strategy starts with enouncing 3 basic principles:[14]

1. The same core values, laws and norms that apply in the physical world apply also in the cyber domain. In particular, any information sharing for the purposes of cybersecurity, when personal data is at stake, should be compliant with EU data protection law and take full account of the individuals' rights.

2. The Internet is a public or collective good that should be available to and accessible by all.[15]

3. The governance model for Internet should be democratic and cybersecurity

[13] In Nov. 2015, 47 states had ratified it, and a further 7 only signed it. Many non-European countries – such as Brazil, India, China and Russia- declined to adopt it on the grounds that they did not participated in its drafting, it was inconsistent with their security culture and it would undermine their sovereignty. In 2011, the head of data protection and the cybercrime division of the Council of Europe said it would be impossible to negotiate a treaty such as the Budapest Convention today.
http://www.pcworld.com/article/244407/despite_controversy_cybercrime_treaty_endures.html

[14] http://eeas.europa.eu/policies/eu-cyber-security/cybsec_comm_en.pdf

[15] For the EU, access to Internet is a fundamental right whereas for the UN, it's not a right but a means to exercise other rights.

policy should be a shared and multi-stakeholder responsibility. [16]

The Strategy then defines five strategic priorities:

1. Achieving overall *resilience* of the EU (including EU institutions)
2. Fighting *cybercrime*
3. Developing cyber defence policy and capabilities related to the *Common Security and Defence Policy* (CSDP)
4. Developing *industrial and technological resources* for cybersecurity
5. Establishing a coherent *international* cyberspace policy in order to promote core EU values (EU "cyber diplomacy").

Each of the first three pillars, which deal with cyber capabilities, is respectively associated with an already existing agency, namely:

1. The European Network and Information Security Agency (ENISA), created in 2004 and based in Heraklion (Crete), which offers a platform for inter-governmental cooperation over cybersecurity and has the authority to force Member States to take actions for cyber resilience.
2. The European Cyber Crime Centre (EC3), established in 2008 and operational since 2013, which, along with Eurojust, plays a pivotal role in law enforcement. Hosted by Europol in the Hague, it merges sources and resources for facilitating and coordinating the fight against cybercrime and it provides training as well as operational support for investigations.
3. The European Defence Agency (EDA), which works with the EU Military Staff (EUMS) to improve cyber defence capabilities.

Since an important objective of the Strategy is to harmonise cybersecurity capabilities of European member states, it remains that each EU member state must possess a well-functioning national-level computer emergency response team (CERT), and a competent authority to speak on behalf of the country. The Strategy also aims at strengthening cooperation between the public and private sectors.

The defence part of the EU Cybersecurity Strategy is probably its most interesting characteristic, since defence and security are domains in which EU member states have traditionally been the most protective of their sovereignty. The general principle according to which the EU has no standing military forces, no EU-owned military equipment, and its external operations depend on force contributions from member states also applies to cyber defence: only MS can provide cyber defence capabilities for EU-led operations. The strategy calls nevertheless for concepts, structures, and

[16] See also COM(2009) 277, Communication from the Commission to the European Parliament and the Council on "Internet Governance: the next steps".

capabilities for cyber defence at the EU level, and it defines four major objectives: helping member states (whose level of cyber defence capability varies greatly) to develop cyber defence capabilities related to CSDP; building a EU Cyber Defence Policy framework; promoting civil-military dialogue; developing dialogue with international partners (NATO and other major stakeholders).[17]

The fifth and last priority in the Strategy is the development of EU "cyber diplomacy" - in other words, a policy that can also be projected outwards. Europe has in effect the ambition to be a normative global actor, capable to create an effective and constructive culture of cybersecurity within and beyond the EU. This means, in particular, having an influence in global deliberations on norms[18] and principles for cyberspace behaviour.

The comprehensive Cybersecurity Strategy was accompanied with a *European Directive on Network and Information Security* (NIS Directive). Voted in March 2014 by the European Parliament and Council, the directive requires Member States to put in place a minimum level of national capabilities –in particular NIS national authorities and Computer Emergency Response Teams (CERTs)- to adopt national NIS strategies and cooperation plan, and to mandate the reporting of significant cyber incidents across all critical infrastructure sectors. The directive also states that operators will be liable, regardless of whether or not they carry out the maintenance of their network internally or if they outsource.

The Cyber Defence Policy Framework and EU external missions

Cyberspace is a critical element in the success of EU external missions and operations, both military and (even more) civilian. Thus they all include a more or less developed cyber component (see EU NAVFOR Med/Sophia or EUFOR RCA). Given the strong national differences of skills and cultures in the field, each mission represents a challenge, not only technical but also societal and legal.

This cyber dimension of CSDP missions and operations has been taken into account at the highest decision-making level of the EU: in December 2013, the European Council asked the High Representative to develop a Cyber Defence Policy Framework, with the support of the European External Action Service (EEAS), the Commission services and the European Defence Agency (EDA). Adopted in Nov. 2014 by the European ministers of defence, this Policy Framework is a non-legislative document with both a civilian and military dimension, which clarifies the roles of the various European actors, and which specifies five priority areas for improving CSDP cyber defence:

1. Supporting the development of Member States' cyber defence capabilities related to CSDP.
   The main focus is on developments relating to monitoring, situational

[17] Robinson, N., (2014) 'EU cyber-defence: a work in progress', European Union Institute for Security Studies

[18] On norms, see Healey, J. (2011), 'Comparing Norms for National Conduct in Cyberspace', 20th September

awareness, prevention, detection, protection, information sharing, and forensics analysis. The EDA also works on "pooling and sharing " projects.

2. Enhancing the protection and resilience of CSDP communication networks used by EU entities, particularly the EEAS.

   Efforts are focused on the development of a unified doctrine of cybersecurity and defence covering all CSDP missions and operations at the strategic planning level. The EU Military Staff has recently launched the revision process of the EU concept for the cyber integration to military operations.

3. Promotion of civil-military cooperation and synergies with wider EU cyber policies, relevant EU institutions and agencies, and the private sector.

   Important objectives are to align military R&D efforts with civilian programs, and to improve the integration of a cyber dimension to programs with a dual dimension (SESAR, Galileo).

4. Improve training, education and joint exercises.

   One objective is to develop a common culture of cybersecurity and cyber defense at the European level, and to diffuse it to the whole chain of command of CSDP operations and missions. Training needs requirements are also being elaborated.

5. Enhancing cooperation with relevant international partners, such as NATO.

At the EU and national levels, a lot of work is currently being done to update both doctrine and operational means. The EDA, in particular, works on the identification of needs in terms of critical assets. Required capabilities are not only material (sensing capabilities, hard and software, secured IT networks) and human (skills and expertise), but also organisational. Once identified, needed capabilities are compared to the actual state of play, in order to fill the gaps.

A lot of efforts are devoted to other crucial elements, such as training and threat assessment planning (establishment of procedures, feed-backs from previous experiences, etc.). An important objective is a better cyber integration between the Crisis Management and Planning Directorate (CMPD) and the Civilian Planning and Conduct Capability (CPCC). A lot of conceptual work is done in parallel to develop a EU agreed concept on cyber defence and to integrate it at the doctrinal and international levels.

The cyber space dimension is also fully taken into account in the planning of EU external missions and operations, both civil and military. For implementing the EU common security and defence policy (CSDP), EU civilian and military missions and operations need strong protection against cyber attacks. Hence it is integrated from the start in the planning process. How can risks be treated? What are the critical assets? What is the necessary level of training for an operation? These are some of the questions in the early preparatory phase. Before the operation, what is crucial is the information and training

of participants, and many efforts are performed to ensure cybersecurity awareness of personnel of all ranks. Needed cyber defence capabilities then vary according to the operational phase. During the phase on the ground, the most important tasks are to ensure informational and networks security. This implies threat intelligence, incident response support and information sharing. After the mission, debriefing and feedback are key to draw lessons and update the cyber landscape. All missions are backed by a CERT, with a possible support of the CERT-EU.

IV The specificities of the European cybersecurity policy

The EU cyber security policy diverges both from policies pursued in EU member states and from policies that are being developed in the rest of the world in several important respects. We will briefly examine three of them: the nature of the "cyber power", the governance model, and the respect of fundamental rights.

Cybersecurity and the conception of "cyber power"

The EU, in conformity to its core norms and values, doesn't develop the kind of hard and offensive cyber power concept pursued by those states, democratic or not, that approach the issue of security in cyberspace through the logic of national security and cyber superiority. The EU approach is basically legalistic and protective. The EU cybersecurity concept concentrates on fighting cybercrime, and on resilience to ensure rapid recovery from cyber attacks. EU capability development focuses on soft power capabilities, i.e. building capacities that enable detection, response and recovery from sophisticated cyber threats. In the defence/military field, the EU is solely engaged in cyber self-protection and assured access to cyber space to enable its operations and missions. Offensive capabilities, when they exist, are not developed nor deployed under the EU banner.

This is a crucial difference with the concept defined in the US after the terrorist attacks on September 11th 2001,[19] and with approaches carried on by other crucial state players, such as the Russian Federation or the People's Republic of China, all widely suspected of sponsoring various forms of cyber attacks for political purposes. It also contrasts with choices made by a majority of individual EU member states, which allocate significant budgets and personnel to develop cyber-offensive capabilities.

Governance models

Governance issues are crucial, since they strongly influence forms of social, economic and political control. Till recently, the virtual world was essentially an open arena with little established rules. Given the complexity of the cyberspace and the number of actors

[19] The US National Strategy to Secure Cyberspace was published in 2003 as a part of the overall National Strategy for Homeland Security.

involved in its management and use, most of its control came from business and civil society, and the role of states was limited to indirect rather than direct influence. The development of cyberspace, however, made the issue of its governance the subject of intense debates, in particular in relation to the role of governments. While there is a quasi-consensus on the need for more effective governance, there is no agreement on the form it should take.

Governance models pushed by states are very disparate. They oppose, broadly, multi-stakeholder models to governmental models. On the one hand, a number of non-European countries, such as the US, Japan, Canada and Australia, share with the EU the vision of a multi-stakeholders governance. They consider that traditional top-down state-centred models are ill suited to decentralised, global, publicly shared but largely privately developed communication networks. They do not agree, however, on the list of relevant stakeholders. While the EU recommends the inclusion of all players -from citizens to governments- the US argues for a predominantly non-governmental model with a strong participation of the business sector. The US government, which insists on regulating cybersecurity through technological standards -as it views such standard setting as commercially beneficial to the US economy- calls for industry-government cooperation over a standardization of the Internet's security that would be industry-led.

On the other hand, the multi-stakeholder approach is highly contested by those countries, such as Russia, China, Iran and India, which defend both a centralised and intergovernmental approach. Arguing that Western countries –in particular the US- are holding too much power over the management of the Internet and themselves are under-represented in the actual global Internet governance institutions (Internet Corporation for Assigned Names and Numbers, Internet Governance Forum, etc.), they plead in favour of much more governmental involvement in cyberspace, and they want the Internet to be governed at the international level by inter-governmental organisations, such as the International Telecommunication Union (ITU), a UN agency. The Shanghai Cooperation Organization (SCO) members (China, Kazakhstan, Kyrgyzstan, Russia, Tajikistan and Uzbekistan), for instance, have an agreement in place – the International Information Security Agreement – that emphasizes a primary role for the state in controlling information technology, and managing risks and threats.

The problem, however, is more complex than a binary choice between private or public, freedom or control. While the world's (US) major technology firms have already moved into all the cyberspace regulating bodies in order to push ahead their private interests, demographic and economic factors tend to increase the weight of countries where freedom is an elusive and unsettled concept. Any move away from the current status quo that would strengthen interstate regulation, however, would lead to the fragmentation of cyberspace and to forms of closure and control that would be not compliant to the original spirit of the Internet, nor the respect of fundamental rights.

The EU, given its unique features, has in theory the potential to be a model for other regions of the world. In the field of cybersecurity, it is a remarkable full-size "institutional laboratory", which must constantly find compromises and trade-offs between contradictory actors, principles, instruments and interests. Because it is genuinely committed to promote an alternative integrated model in Europe, it had to move beyond the traditional top-down state-centred approaches and to adopt a multi-stakeholder approach, making it possible to bring together suppliers, users, public sphere, academics and civil society representatives. The EU also built a consistent and comprehensive governance model, with a decentralized structure in which different agencies and institutions are responsible for different aspects of the digital world, and political and legal control is respectively exercised by two major institutional players: the EU Parliament and the European Court of Justice, which play an essential role in avoiding the capture of the regulatory game by economic lobbies, political leaders or technological experts, ensuring a balance between cybersecurity, public interest and other legitimate economic, commercial or regional interests, and defending the European citizens' rights and freedoms.

While the EU has the claimed ambition to be a normative power in the field of cybersecurity, however, its records at the international level are disappointing. This poor record is due partly to its failure to conduct discussions and defend its values both in multilateral negotiations and in bilateral cyber dialogues with its closest partners -the US and NATO- but also partly to its insistence, at least on the paper, on the defence of fundamental rights. This emphasis, which is perhaps its main distinctive characteristic, is also the main obstacle to convergence with the rest of the world.

Fundamental rights' protection

In the cyber domain, the main difference between the EU and other approaches is the attention paid to the respect of civil liberties and the rule of law, including international law, and to the promotion and defence of fundamental rights. While the EU, which cannot depart from the principles of the European Charter of Human Rights, is preoccupied with balancing cybersecurity with the protection of such rights, individual countries –both outside and inside Europe- are more ready to accept derogations for reasons of national security, particularly as regards data protection and right to privacy.

In many countries, including democratic ones, obsession with security often tends to remove limits of what is acceptable in a democracy. A typical case is the US, where after the Sept. 11 attacks, the Administration set up a legal framework that furnished the base for mass surveillance programs. The Patriot Act, in particular, tremendously increased the powers of US security agencies, which soon expended their activities, in a total opacity, from fighting terrorist networks to widespread surveillance of both the American and world population.

The EU, by contrast, officially set up rules offering higher standards of guarantees and preservation in terms of data protection and respect of privacy. This is all the more

remarkable that not all member states spontaneously follow that line. As we know from the Edward Snowden's revelations, a number of EU Member States (in particular the UK and Sweden) were complicit in mass data surveillance of European citizens, in contravention of EU laws on privacy/data protection, and codes of conduct among Member States. Such activities, incidentally, existed long before the "War on Terror" launched under Bush administration. It was for instance the revelation, during the Cold War, of a secret Anglo-American global electronic surveillance system of international communication networks,[20] which pushed the European Parliament to publish in July 2001 a first critical report on the subject.[21]

Within Member States, battle against cybercrime and terrorism is also a serious source of concern about privacy and freedom protection. Most national politicians, for electoral reasons, systematically call for more surveillance and biometrics, and a number of national laws and practices in EU member states appear to be illegal with regard to democratic rights. In France, for instance, after the terrorist attacks of 2015, the government took advantage of the emotional context to impose an extensive domestic surveillance program on the model of the US Patriot Act, with the argument that it is impossible to ensure both people's security and full respect of their privacy, as if security and freedom were part of a zero sum game strategy.

The European Commission itself has not always been exemplary in arbitrating between security and fundamental rights. In several cases, it has been disapproved by the Parliament or the European Court of Justice, bastions for the protection of European values, particularly in partnerships between the EU and the rest of the world. An example is the Safe Harbour case, in which the Commission was disavowed by the ECJ (see below). The sentence was a great victory of fundamental rights over not only profit and business, but also mass surveillance programs. As a European MP declared, however: "We can not always expect judges to repair sloppy legislative work by politicians looking for easy and popular measures".[22]

Indeed, to a large extent, the EU cybersecurity policy has been a reactive rather than a proactive policy. Normative texts set up by the EU in the field of cybersecurity have often appeared as reactions to external circumstances. They reflect tensions between two opposite aspirations, security and freedom, between which arbitration is influenced partly by the tumultuous relationships in that field between the US and Europe, and partly by emotional reactions after terrorist attacks. The successive revelations of the US surveillance activities of European citizens, for instance, had an undisputable norm-productive effect. It brought the issue of rights and democracy under closer scrutiny,

[20] The so-called Echelon espionnage program, also known as the "Five Eyes", was a global system for the interception of private and commercial communications that operated on behalf of the five signatory nations (Australia, Canada, New Zealand, the UK and the US) to the UKUSA Security Agreement.
[21] Schmid, Gerhard (11 July 2001). "On the existence of a global system for the interception of private and commercial communications (ECHELON interception system), (2001/2098(INI))" (pdf – 194 pages).
[22] Sophie in't Veld. http://europe-liberte-securite-justice.org/2015/10/09/safe-harbor-is-anything-but-safe-when-a-citizen-and-the-ecj-overcome-the-institutions/

and increased pressure within the EU to ensure the respect of European citizens' rights online, both domestically and abroad.

The Safe Harbour case

Promoted by the EU Commission, the so-called Safe Harbour Agreement, signed in 2000 between the US and the EU, enabled American companies to compile data generated by their European clients online. During its long negotiation, two different approaches to online data protection clearly emerged: that of the United States, viewing privacy mainly as a consumer protection issue; that of the EU, seeing it as a fundamental right, of the same rank as freedom of expression. In spite of repeated calls for the repeal of Safe Harbour from the European Parliament and legal experts, the Commission sustained Safe Harbour.

After the Agreement was signed, the gap between the European and the American approaches on the topic widened, due partly to the evolution of the US law enforcement and national security policy towards a more interventionist approach after the US PATRIOT Act of 2001, and the amendments of the Foreign Intelligence Surveillance Act (FISA) of 2008, and partly to the entry into force in 2009 of the Lisbon Treaty, the European Charter of Fundamental Rights, which acquired the status of primary law, meaning that all the EU legislation, including the Commission's decision on Safe Harbour, was now subject to the principles and the rights laid down in the Charter (in particular art. 7, 8, and 47, which respectively state the principles of respect for private and family life, protection of personal data and right to an effective remedy and to a fair trial).

It was in that context that in 2013 Edward Snowden revealed how American and British intelligence agencies had unfettered access to people's online activities. By so doing the NSA whistleblower provided a ticket to courts both to American and European citizens. In the US, while a federal court of appeal declared the telephone surveillance program outlawed, the US Senate demanded clear limits to this phone surveillance program. The adoption of the US Freedom Act was for the US legislator a first step in the reform of US surveillance programs. In the EU, in Oct. 2015, the European Court of Justice invoked the supreme nature of the fundamental rights and freedoms laid down in the Charter to disavow the EU Commission and declared Safe Harbour invalid.

In the other direction, an illustrative example is the hesitancy of the European Union in its approach to terrorism. While it is officially refractory to the US military logic of the "war against terror" and it claims a different and more balanced approach to the question, the recent development of anti-terrorism strategies and tools shows a worrying convergence with US practices and visions. In the cyber domain, this alignment has been formalized by several recent agreements between the US and the EU, such as

the processing and transfer of PNR (Passenger Name Records or PNR data), which had previously been rejected by the European Parliament.

Conclusions

The digitalisation of our societies creates new forms of vulnerability and new potential threats, as ill-intentioned people can relatively easily gain access both to sensitive information and to the operation of crucial services. Critical infrastructure systems are complex and therefore bound to contain weaknesses that might be exploited. Malevolent actors -which include states as well as criminals and terrorists- can, at least in theory, approach targets that would otherwise be utterly unassailable, such as power grids, air traffic control systems, or public services, that might be attacked to inflict human or material destruction. So far such cyber attacks have not killed people, but this could come in a relatively near future.

Such threats are addressed by cybersecurity policies, whose effective implementation depends not only on state actions, but also on cooperation across the public-private divide, and on coordination between policy areas and international institutions, especially the EU.

Though cyber policies are mainly national policies, the EU has an important role to play in the field, which goes beyond coordination and harmonisation of national policies. In recent years, it has been working to implement a consistent, balanced and overarching cybersecurity strategy, built on internal resilience and EU core values. The EU declared ambition is to make the EU's digital environment not only the most secure, but also the most respectful of the citizens' fundamental rights in the world. This is a real challenge, given the difficulty to find a satisfactory and sustainable balance between security, freedom and protection of citizens' fundamental rights.

The EU objective to develop a cyber 'soft' power privileging defence, resilience and civil society sharply contrasts with national cybersecurity policies that are developed both inside and outside Europe. In Europe, where governments tend to play on emotional reactions to terrorist threats to support traditional national security approaches, some uncertainty still remains over Member States' buy-in for such a common EU approach. In the rest of the world, major cyber players (in particular the USA, Russia and China) have different concepts, cultures and logics on these matters, particularly regarding norms for cybersecurity behaviour. The EU and U.S. approaches to cybersecurity, for instance, in spite of some common features, present important differences, as the "war on terror" launched by the Bush administration led not only to war doctrines and preventive police guided by technological determinism, but also the set up of a legal framework that today is accused to have furnished the base for mass surveillance programs.

Yet, an important aspect of the EU "cyber diplomacy" is the support of international discussions on definitions of behaviour norms in cyberspace, which if they were agreed upon internationally would help to improve global security and state behaviours' transparency and predictability. The EU's poor record in terms of projecting its normative vision for the governance of the Internet and cyberspace in the global arena is problematic, since it hampers its efforts to promote a consistent and comprehensive governance model in the area of cybersecurity, characterised by integrity and dedication to genuine freedom in cyberspace.

How to find a compromise capable to satisfy opposite exigencies (security and rights protection), which constitute complementary imperatives laying at the root basis of democratic systems? If it is certainly wrong to regard the negative impact of communication technologies as uncontrollable, it is also wrong to imagine that one can bring them completely under control. Too much security kills security, and some policy responses to cyber threats are just as worrying in the long term as the evils to which they pretend remedy, as they somehow remind the way some immediate dangers perceptions have led to the erosion of democracy at other times in European history.