# 10

# Appendix B: Conceptualizing Cyber Security from the EU Perspective

In 2004, ENISA (European Network and Information Security Agency) was founded in order to facilitate "best" practice among Member States with regard to cyber security policies with regard to EU's Information Society agenda. In 2007, due to DDoS (Distributed Denial of Service) attacks on the public infrastructure of Estonia, the EU along with NATO and other related actors considered changing their approach. As a result, the EU's policy has been developed within the light of the Europe 2020 strategy. The European Commission (2013) and its Principles and Guidelines for Internet Resilience and Stability (2011) focus on the significance of global partnerships to address both military and civilian aspects of cyber security challenges.

According to the EU Cyber security strategy, the Internet must be kept protected and "open and free" based on the same values and principles that the EU considers for offline space (EU Cyber security Strategy). EU Cyber security Strategy and its Directive on Network and Information Security (NIS Directive) were published on 7 February 2013 to require the reporting of significant cyber incidents across all critical infrastructure sectors (NIS Directive, 2013). For the first time, the EU tried to specify priorities with regard to the protection of cyberspace via means of this strategy as previously there was no coordination with regard to the construction of an effective security ecosystem for cyberspace (Klimburg and Tirmaa-Klaar 2011).

This section will be structured as follows: After a brief overview of the conceptual landscape of the EU's cyber security development, the suggested tools for cyber security policy of the EU will be explained. Next an overview of the EU's way of dealing with cyber security threats will be explained. The final section will provide recommendations for the EU's cooperation with other states on cyber security in the future.

## 10.1 Concepts and Approaches of the EU's Cyber Security Policy

The existing body of academic literature with regard to the EU's action in cyber security is scarce as most of the available work focuses on the United States and other regions (Kshetri, 2013), with no in-depth theoretical analysis of the EU's cyber security policy. Various approaches such as managerial and strategic (Libicki 2007, 2009; Clarke and Knake 2010), historical (Carr, 2009) and other approaches that focus on terrorists (Wiemann 2006; Colarik 2006) have been used. While the emphasis of such approaches has been more on recent cyber threats and how to establish the "cyber peace" (Clarke and Knake 2010), other theoretically and methodologically driven works used innovative mixed-method (Deibert et al. 2011), regulatory (Brown and Marsden, 2007) and other approaches that try to evaluate the extent of securitization of cyber policy (Dunn, 2007, 2008; Bendrath et al. 2007).

Cyber power has been so far one of the most frequently used concepts with regard to cyber security (Klimburg and Tirmaa-Klaar 2011; Betz and Stevens 2011; Klimburg 2011; Nye, 2010; Kramer et al. 2009). While Nye (2010) defines cyber power as the ability to utilize the digital pace to create an influence and gain advantages in other operational contexts (2010, p. 4) he makes a distinction between information and physical instruments, as well as soft and hard power in cyber space, and provides examples of how they can be used both outside (extra-cyberspace power) and inside (intra-cyberspace power) (See Table A10.1).

Other scholars such as Betz and Stevens (2011, p. 44) acknowledge the fluidity of cyberspace and mention that and that various non-state and state actors, ranging from states to citizens, global networks, and organizations, can have an influence at any point in time in order to exploit the possibilities

**Table A10.1** Instruments of power in cyberspace

| | Intra-cyber Space | Extra-cyber Space |
|---|---|---|
| Information instruments | Soft: Set standards and norms | Soft: Public campaign to influence opinion |
| | Hard: Denial of Service Attacks | Hard: Attack SCADA systems |
| Physical instruments | Soft: Infrastructure to support activists of human rights | Soft: Protests to name and shame cyber providers |
| | Hard: Government controls over enterprises | Hard: Cut cables or bomb routers |

*Source*: Nye, 2010.

offered by cyberspace. As a result, they conceptualize the cyber power in four distinct forms:

- *Compulsory:* This occurs when one cyberspace actor makes use of direct coercion to change the behavior of another actor (hard power such as attacks on FBI systems);
- *Institutional:* This refers to one of the actor's Indirect control by means of formal and informal institutions (soft power such as setting norms);
- *Structural:* This refers to a control type which aims to maintain the existing structures and enable or limit the actions of the actors with regard to those with whom they have a connection (soft power regarding how cyberspace can enable or limit the actions of actors);
- *Productive:* This refers to the definition of the "fields of possibility" that limit or enable social action (soft power such as a states' construction of the "hacker" as threat) by means of discourse.

According to Klimburg (2011), cyber power has the following other crucial aspects:

1) Coordination of policy and operational aspects across governmental structures;
2) Policy coherency through international alliances and legal frameworks;
3) Cooperation among non-state cyber actors.

In opposition to Nye (2010), Klimburg (2011) asserts that the last one is the most significant one as most of the control is exerted by civil and business society due the nature of the cyberspace and the state's capability is restricted to indirect influence. Based on the Model of Integrated Capability (Klimburg and Tirmaa-Klaar 2011), Klimburg (2011) emphasizes the need for a holistic approach to cyber security, in other words a soft-power approach which is focused on the inward is fundamental for the creation of a "whole of nation" of cyber capability' (2011, p. 43). Although the European Commission (2013) included some of these scholars' recommendations, it is not certain whether "hard" cyber power considered in EU's conventional national security terms is actually aligned with the EU's core values. This is a crucial point given the revelations of post-PRISM (e-spying) that certain EU Member States such as Sweden and the United Kingdom were complicit in mass data surveillance of citizens in contravention of the EU laws on data protection among "friends" in Europe.

Within the light of this information, it can be argued that the EU needs a security policy based on resilience approach (Christou, 2015) and a specific kind of soft cyber power based on Klimburg's three aspects including productive and institutional cyber power, rather than the conventional and hard cyber power often exercised by democratic and authoritarian states, based on the logic of cyber sovereignty. In the post-Snowden era, this is even more imperative as the consequences of a mindset of "national security first" have been in sharp contrast with the vision of EU's open, safe, and secure cyberspace. In this regard, Dunn-Cavelty (2013, p. 3) states that a special type of "soft" power driven by core values and internal resilience should be developed by the EU to make sure that its normative vision with regard to the cyberspace's governance is obtained within the global arena.

## 10.2 The EU Approach to Cyber Security

Over time as the EU's approach to cyber security evolved in an *ad hoc* and fragmented manner, several strands of cyber security "policy" emerged which can be categorized as in Table A10.2:

According to Robinson (2013), given the complexity of the cyber security domain, and the difficulty for the design of a coherent internal EU policy, these strands entail the following aspects:

- Legal (enforcement),
- Economic (Internal Market)
- Security (CSDP).

Furthermore, the Cyber security Strategy also includes both the development of technological resources for cyber security and the establishment of policy for cyberspace in order for the EU to contribute to its the fundamental values. (Robinson, 2013):

**Table A10.2** Strands of EU's cyber security policy

| Policy Strand | Responsible Institution |
|---|---|
| Cybercrime and cyber attacks | Directorate General Justice and Home Affairs |
| Network and Information Security (NIS):<br>a) Critical Infrastructure Protection (CIP)<br>b) Critical and Information Infrastructure Protection (CIIP) | Directorate General Connect (previously DG Information Society) |
| A cyber defense element | European External Action Service (EEAS) |

*Source*: Robinson, 2013.

Based on the normative foundation of the EU approach, the global Internet is regarded as a collective or public good which should be made accessible and available to all (European Commission, 2013; European Principles and Guidelines, 2011). So the use of the Internet should only be constrained when instruments and measures are used to provide harm to others. An effective cyber security strategy should take as its basis the main norms as stated in EU's Charter with regard to its Fundamental Rights (European Commission, 2013). Thus, the main EU values and norms are at the core of both online and offline activity, as stated in its Cyber security Strategy.

According to the European Commission (2013), the governance model of its cyber security policy should be based on multi-stakeholderism which arises due to the complex interactions among several actors using and managing the Internet. Some states such as Iran, Russia, China, or India held the opinion that due to the excessive power of the United States over the management of the Internet these countries themselves are under-represented in current Internet governance institutions such as the ICANN (Internet Corporation for Assigned Numbers and Names) or IGF (Forum for Internet Governance).

As any of these principles on EU cyber security policy cannot exist in a vacuum, a specific type of public–private partnership is supported under this multi-stakeholder umbrella. Therefore, while the appropriate forms and modes of governance (i.e., incentives) should be agreed by public authorities in consultation with related stakeholders, the private sector plays an important role in day-to-day governance of the Internet (European Principles and Guidelines, 2011). If there is any global disagreement with regard to the role of technical standards, data protection, who should regulate the Internet, and the appropriate legal conventions for fighting cybercrime (e.g., the Budapest Convention), these can undermine any effort to develop a secure cyberspace for everyone. In the post-Snowden era, an increased support for the Governmental Advisory Committee in ICANN was provided by the EU, by assigning it a greater decision-making role in policy on Internet governance.

## 10.3 Progress and Challenges of the EU Cyber Security Strategy

As Robinson (2014) states, in comparison to the United States, China, or Russia, whose main focus is on a national security (threat) logic and hence deterrence and militarization constitute their central strategy (hard power),

the EU is focused on building resilience to enable fast recovery from cyber attacks, developing the required capacities to resist cyber attacks, and fighting cybercrime (soft power). For the EU, those priorities that focus on non-military aspects which aim to create partnerships for the development of an effective cyber security culture within and beyond the EU are more important that its military and intelligence infrastructures (Bendiek, 2014). include not only dialog, incentives, platforms for cooperation and coordination, and voluntary arrangements (to ratify the Budapest Convention), but also more formal requirements, such as the suggested NIS Directive to protect both the privacy and data of its citizens. Yet, it is not known which of these instruments provide the EU with the opportunity to create effective productive (soft) and institutional cyber power.

With regard to the preparation of its Cyber Defense Policy Framework, the EU so far developed bilateral relationships by means of participation in international platforms such as the London conference and appropriate international fora (OECD, ICANN, ITU, IGF), as well as international organizations such as NATO.

On the other hand, there have been some issues with the CoE (Budapest) Convention on Cybercrime as it was not implemented by all Member States across Europe. Besides, some countries such as Russia and China oppose ratifying the Convention as they are concerned that national security culture would be undermined because Internet users in these countries are often the alleged source of many cyber security attacks (Goldsmith, 2011).

Being members of SCO (Shanghai Cooperation Organization), Russia, China, Tajikistan, and Uzbekistan proposed in September, 2011 that the UN Secretary General should establish a dialog about the new "Code of Conduct for International Security" with the purpose of reaching an agreement on international norms of behavior for the Internet. Although at first sight, its main principles (Appendix C) are in alignment with what is being advocated by the EU with regard to full respect for rights and freedoms in cyberspace, an in-depth look reveals that rather than supporting a multi-stakeholder approach to cyber security, the commitment to prevent other states from using core technologies to threaten other countries' security is underpinned by a sovereign logic of control rather than freedom (Gjelten, 2010).

The promotion of the UN to take a more active role in Internet governance, where China has much more influence and weight in terms of voting behavior, could lead to a potential separation of national Internet spaces, rather than multi-stakeholder governance. In addition to the perceived dominance of the United States in controlling the Internet, given the SCO

members' commitments to restrict information flows in case of any impact upon their security culture, the main concerns are about repressive regimes' excuses to restrict access to independent external news sources, as in the case of the Arab uprisings (Gjelten, 2010). As some scholars argue, this might also be used as a justification to develop draconian laws on access and dissemination of information which might threaten "national security" (Healey 2011b; Bendiek, 2014). Finally, the fact that states such as Russia and China which are seen to be at the center of cyber conflict do not support a commitment to control patriotic hackers is regarded as another concern. Besides, no Code calls for all states to sign up and be bound by the laws of armed conflict which raises many questions with regard to the legitimacy and proportionality of certain targets (Christou, 2015).

## 10.4 Conclusion

If the aim of the EU is the establishment of deeper cooperation with other nations within the context of cyber security in the future, platforms (e.g., the Task Force) should create an effective agenda that reflects the differences between the EU (soft power) and other countries such as China or Russia (hard power). Yet, there should not be any compromise in the principles and norms of these countries with regard to their Internet policies. Although this may sound as being too difficult to accomplish it is not impossible given EU's increased emphasis on cyber security along with its evolving cyber security strategy.