elf

INSTITUTE FOR POLITICS
AND SOCIETY

Cybersecurity

The Public-Private Dilemma

POLICY BRIEF | May 2017

Cybersecurity

The Public-Private Dilemma

Policy Brief – Jan Klesla and Kelsey Beckmeyer, May 2017

This is a policy brief to the event International Security, Strategy and Cyber Security that was organized by European Liberal Forum and Institute for Politics and Society on 30 March 2017. The speakers were Lior Tabansky, PhD candidate in Cybersecurity at Tel Aviv University's Blavatnik Interdisciplinary Cyber Research Center, Zuzana Duračinská, Computer Security Specialist at CZ.NIC, and Martin Rehák, Principle Engineer, CISCO. The roundtable was moderated by Jan Klesla.

The roundtable discussion was organized by the European Liberal Forum (ELF) with the assistance of the Institute for Politics and Society, and co-funded by the European Parliament. The European Parliament is not responsible for the content of the program, or for any use that may be made of it. These views do not necessarily reflect those of the European Parliament and/or the European Liberal Forum.

The government's role in cybersecurity

National security is the responsibility of the state, but where are the boundaries of its jurisdiction when national security is threatened in cyberspace? How will the public and private sectors respond to cyberattacks, and whose responsibility is their cybersecurity?

Cybersecurity and data protection has become a priority for nations over the last decade. Governments, corporations and individuals are becoming more and more reliant on technology and securing data has been an unending challenge. Security incidents such as hacks, viruses and software failures put vital data at risk ("Improving cyber security across the EU", 2016). Such incidents are becoming more frequent and innovative in how information is targeted.

In order to mitigate the risk of cyberattacks, the EU and its member states are taking steps to increase cybersecurity. With the assistance of cyber researchers and developers, governments are looking for ways that cybersecurity can make security frameworks more resilient, adaptable and reliable (Greengard, 2016). However, the government's leadership role in protecting data increasingly raises concerns from private businesses and corporations about whether these new measures might actually heighten vulnerability, rather than improve protection.

This paper will consider laws in the EU and Czech Republic to understand the role governments play in securing public data as well as private data. We will consider the implications this holistic approach has for private security. Should we expect government involvement to heighten cybersecurity, or does its involvement potentially put private data at risk?

European Union objectives and legislation

In 2013, the European Commission (2017) published a list of objectives for cybersecurity, which include:

1. Increasing cybersecurity capabilities and cooperation
2. Making the EU a strong player in cybersecurity
3. Mainstreaming cybersecurity in EU policies

These objectives aim to raise all EU Member States to the same level of security and technological development. They also focus on promoting European engagement in innovation related to enhancing cybersecurity techniques, while providing equal access to related technologies. The European Commission (2017) strives to embed cybersecurity into all future policies as technology achieves new heights.

In an effort to meet their objectives, the Commission initially proposed a directive for network and information systems (NIS) security. While not legally binding, this directive aimed to develop a unified cybersecurity methodology throughout the Member States (European Commission, 2017).

On 7 December 2015, the European Parliament adopted the Directive, which became legally binding in July 2016. As of August 2016, the Member States were provided 21 months to develop legislation meeting the Directive's new requirements.

As it is written, the new directive focuses on three main areas (European Commission, 2017):

1. Member State preparedness, which requires a Computer Security Incident Response Team (CSIRT) as well as a national NIS Authority.
2. Cooperation, which establishes a 'Cooperation Group' to facilitate actions regarding cybersecurity and information sharing between and among the Member States and a CSIRT Network.
3. Promoting a culture of security with all actors involved including businesses and individuals.

In addition to unilateral Member State compliance, the new law dictates that other "key digital service providers" must also act within regulative boundaries (European Commission, 2017). This means that all search engines, cloud services and other online marketplaces that operate within the Member States, must comply with the new law.

The Czech Republic's compliance measures

The Czech Republic was the first EU member state that adopted legal framework for the cybersecurity in form of binding law. Cybersecurity Bill (Act no. 181/2014) was passed after long discussion between public and private sector. The efforts to secure Czech government and cyberspace against cyberattacks strengthened after massive DDOS in 2013. The main issue has been the liability for potential damages caused by measures adopted by public authority, e.g. shutdown of part of the network. After the bill came to force, National Security Authority (NBÚ) took over the competences from the Ministry of Interior and built the National Cyber Security Center that operates GOVCERT (Government Computer Emergency Response Team), which is mainly responsible for the defense of public servers and websites. Private Czech National CSIRT (established 2011) operates on the basis of a public contract with the National Security Authority.

To comply with the European Parliament's directive Czech Government introduced a bill amending the existing law on cybersecurity (Národní bezpečnostní úřad, 2016). Moreover, the bill would assign the Military Intelligence Service (VZ) new powers alongside the current system of GOVCERT (that will separate from NBÚ) and CSIRT. There is a difference made between "cybersecurity" (which remains with the

National Security Authority) and "cyberdefense" that may also include retaliatory and pre-emptive strikes in cyberspace. To perform these new powers, the Military Intelligence Service was given authority to install devices to the core network of ISPs.

The bill has been controversial on the grounds that it potentially permits governmental access to customer accounts without direct consent. It has been met with particular protest from mobile operators who are apprehensive about allowing the state access to such enhanced power. The central concern here is, again, whether the bill would allow the government to better protect the public, or actually compromise its security.

Securing private data in the public realm

To determine appropriate private-public participation toward pursuing cybersecurity goals, we must define the roles of the state and private sector. In terms of cybersecurity there is considerable overlap and nuance in both areas, compared to their traditional boundaries. According to Eichensehr (2017, p. 470), "the public-private cybersecurity system is characterized by the surprisingly important, quasi-government role of the private" on one hand, while government correspondingly "has become a literal market participant."

The ambiguity of roles related to this particular relationship leads to concerns from the private sector when the state pursues increased control over national cybersecurity. The new directive and subsequent Czech bill both contribute to reduce the public sector's autonomy to secure and protect data. The question remains, however, whether this approach will actually increase the public-sector vulnerability through its dependence on governments, or whether the state's involvement in data protection will benefit all parties.

The private sector has been vital in developing and enhancing cybersecurity technologies and methodologies, which they have traditionally shared with governments via contracted work (Bossong, & Wagner, 2016). Some of the most cutting edge security measures available are developed by private businesses and corporations (Bossong, & Wagner, 2016). New legislation must work to preserve this vital symbiosis. Being at the forefront of cybersecurity may rely on the state's cooperation with private entities as well as their ability to incentivize companies.

At the same time, heightened governmental control over cybersecurity may appeal to some private companies. By ensuring a standard level of protection, all businesses and companies are guaranteed protection equal to that of vastly larger, wealthier ones. If the quality of protection is high enough, companies both large and small will be protected from cyberattacks—at levels that many could otherwise not afford.

The overall dilemma

While the Czech government is very likely to pass the proposed bill, a few questions remain. First, could the quality of state-run cybersecurity systems ever be high enough that all public and private entities win from this arrangement? Even with the most state of the art, multi-tiered cybersecurity system, having all of the data under the same umbrella may allow cyber attackers to access more information than when data was decentralized.

Second, the question of why the government needs access to our private information arises. The rhetoric that governmental cybersecurity would work to intervene attacks and protect citizens is dubious. Through examples such as the debacle with the National Security Agency (NSA) in the United States, we see that the government does not always work in the interest of the people. Therefore, allowing the government unlimited access to personal data may infringe on personal liberties.

Government interests, rather, lie in protecting themselves, and many governments will go to great lengths to ensure protection. They invest substantial resources into securing and mitigating cyberattacks. Due to this high level of scrutiny, might pooling your risk of attack with government resources be worth potential compromise?

Both sides present valid questions and concerns, which should be addressed within more detailed legislation or a Memorandum of Understanding with private partners. There must be clear delineation of what the government can and cannot access without explicit consent.

Finally, it is important to note that not all Member States have the financial capability to access the best cybersecurity available. Through working together, the EU could pool resources from each country to develop a multi-national system to provide protection to all Member States and their residents.

Resources

Bossong, R., & Wagner, B. (2016). A typology of cybersecurity and public-private partnerships in the context of the EU. *Crime, Law And Social Change*. http://dx.doi.org/10.1007/s10611-016-9653-3

Eichensehr, K. (2017). Public-Private Cybersecurity. *Texas Law Review*, *95*, 467-472.

European Commission. (2017). *EU cybersecurity initiatives*. European Commission.

Greengard, S. (2016). Cybersecurity gets smart. *Communications Of The ACM*, *59*(5), 29-31. http://dx.doi.org/10.1145/2898969

Improving cyber security across the EU. (2016). *Consilium.europa.eu*. Retrieved 3 April 2017, from http://www.consilium.europa.eu/en/policies/cyber-security/

Národní bezpečnostní úřad. (2016). *Návrh na změnu zákona o kybernetické bezpečnosti - transpozice směrnice NIS*. *Nbu.cz*. Retrieved 4 April 2017, from https://www.nbu.cz/cs/aktualne/prohlaseni-a-tiskove-zpravy/1161-navrh-na-zmenu-zakona-o-kyberneticke-bezpecnosti-transpozice-smernice-nis/