Government Information Quarterly 34 (2017) 1–7

Contents lists available at ScienceDirect

Government Information Quarterly

journal homepage: www.elsevier.com/locate/govinf

Building cybersecurity awareness: The need for evidence-based framing strategies

Hans de Bruijn, Marijn Janssen *

Delft University of technology, Faculty of Technology Policy & Management, Jaffalaan 5, 2628BX Delft, The Netherlands

ARTICLE INFO

Keywords:
cybersecurity
information security
cyberphysical system
cyberphysical society
cyber war
Internet of Things
framing
communication
evidence-based policymaking

ABSTRACT

Cybersecurity is a global phenomenon representing a complex socio-technical challenge for governments, but requiring the involvement of individuals. Although cybersecurity is one of the most important challenges faced by governments today, the visibility and public awareness remains limited. Almost everybody has heard of cybersecurity, however, the urgency and behaviour of persons do not reflect high level of awareness. The Internet is all too often considered as a safe environment for sharing information, transactions and controlling the physical world. Yet, cyberwars are already ongoing, and there is an urgent need to be better prepared. The inability to frame cybersecurity has resulted in a failure to develop suitable policies. In this paper, we discuss the challenges in framing policy on cybersecurity and offer strategies for better communicating cybersecurity. Communicating cybersecurity is confronted with paradoxes, which has resulted in society not taking appropriate measures to deal with the threats. The limited visibility, socio-technological complexity, ambiguous impact and the contested nature of fighting cybersecurity complicates policy-making. Framing using utopian or dystopian views might be counterproductive and result in neglecting evidence. Instead, we present evidence-based framing strategies which can help to increase societal and political awareness of cybersecurity and put the issues in perspective.

1. Creating awareness

Although most people seem to consider the Internet to be a safe environment and use it on a daily basis using their smart phones, tablets and computers, there are a large number of attacks on a daily basis. Cyberattacks, hacks and security breaches on the Internet are no longer an exception anymore (Arora, Nandkumar, & Telang, 2006). This number is increasing and organizations are incurring higher costs in dealing with these cybersecurity incidents. Although most cyberattacks are harmless, the impact of some is severe. Cybersecurity breaches can range from no or limited impact to Distributed Denial of Services (DDoS), the stealing of data, manipulation of data, identity theft or even taking over control of systems and harm the physical world.

With the adoption the *Internet of Things* (IoT) in daily life, an increasing number of physical objects feature an IP (Internet Protocol) address for internet connectivity and use the Internet for communication (Hernández-Ramos, Jara, Marın, & Skarmeta, 2013). Information and communication systems and the physical infrastructure have become intertwined, as information technologies are further integrated into devices and networks (Ten, Liu, & Manimaran, 2008). In these cyberphysical systems, the greatest impact occurs when an intruder gains access to the supervisory control access and launches control actions that may cause catastrophic damage (Ten et al., 2008). IoT results in a *cyberphysical society* in which everyday life is interwoven with electronic devices. As such, our living society is becoming ever more dependent on cyberspace, a place in which cyberattacks and cyberwars are common. This might occur high risks, as hackers could take-over medical equipment, automatic-driving cars and flight control, which might be even life threatening.

The need for cybersecurity is becoming increasingly important due to our dependence on Information and Communication Technology (ICT) across all aspects of our cyberphysical society. Cybersecurity is essential for individuals, for public and non-public organizations, but guaranteeing security often proves to be difficult. The websites of many governments have limited security (Zhao, Zhao, & Zhao, 2010) and might be easily hacked. The issue of security is not limited to the executive power, but is also relevant to political parties, energy infrastructure providers, water boards, road management, ministries, administrative organizations, NGOs and even sporting organizations (such as the International Olympics Committee), all of which have already been the target of breaches and the stealing of information. The hack on World Anti-Doping Agency (WAPA) released the medical record of Olympic athletes to compromise them, whereas the Stuxnet virus was aimed at harming a nuclear infrastructure. Cybersecurity breaches can thus be said to impact all stakeholders in our society.

Interest in cybersecurity issues often focuses on incidents and how to deal with them after the fact, while a concern for prevention and investments in better cybersecurity have lagged behind. This is surprising in a world where there is a continuing battle between hackers and various societal actors attempting to protect the system. Cybersecurity is

* Corresponding author.
E-mail address: M.F.W.H.A.Janssen@tudelft.nl (M. Janssen).

http://dx.doi.org/10.1016/j.giq.2017.02.007

said to be the new form of war and is viewed as the next platform in modern warfare. Given its importance, why is there so little awareness? and why are we not taking drastic measures to ensure the safety and security of cyberspace?

People have the tendency to select only those parts of a message that they want to hear. One reason is that decision-makers and policymakers, like all people, will react differently depending on objectively equivalent descriptions of the same problem (Levin, Schneider, & Gaeth, 1998). Communication about cybersecurity issues and the urgent need for policies is a difficult endeavour and cannot be easily communicated in a clear and convincing manner. All too often, people point to cybersecurity risk as a means to *futurize* threats to the polity – to create a security *imaginary*, a *fictionalization* that might create a climate of fear (Doty, 2015). Furthermore, the way humans and technology interact, blurs and dissolves the concepts of being 'inside' or 'outside' a cybersecurity space (Leuprecht, Skillicorn, & Tait, 2016). Cybersecurity has been the domain of specialists and experts who are not trained to communicate about the issues. As such, there is a need for message framing, which is strategy for communicating a complex societal problem in such a way that the main arguments are clearly understandable and cannot be easily challenged (De Bruijn, 2017). Although the use of message framing and the need to frame cybersecurity is evident, there is no detailed analysis available.

In this work, we investigate why cybersecurity is not receiving the attention it deserves and how an awareness of the importance of cybersecurity can be created. We start by identifying paradoxes complicating the framing of cybersecurity policies. This is followed by discussing the difficulty of communicating about cybersecurity issues, which has resulted in society not taking appropriate measures to deal with the threats. The challenges are divided into four areas of concern: 1) limited visibility, 2) socio-technological complexity 3) ambiguous impact, related to the strong incentives of market parties to hide the impact, and 4) the contested nature of fighting cybersecurity, for example, measures might need to be taken that violate public values such as privacy. After discussing these issues, we present the need for messages framing, followed by the theoretical background. Finally, we present several frames to deal with these challenges, and call for more research in this emerging area.

2. Cybersecurity: a sea of paradoxes

Policymaking in the field of cybersecurity is currently facing many paradoxes. The choosing of one direction can be at the expense of another direction, whereas there are arguments for going both ways. Cybersecurity politics and policymaking takes place within a complex ecosystems in which stakeholders from a diverse society, the policy field and government must interact with each other. Responsibilities are distributed over many public entities at both the central and local levels, with diverse problems and challenges, making it difficult to initiate collective action. Society consists of diverse players that might want security, but have varied expectations about the role of government in ensuring safety and security in cyberspace. Governments can play minor or major roles in cybersecurity. Politicians must act upon societal needs, develop policies and allocate resources, while the public institutions need to realize the goals set. This might look like a simple relationship, but the situation is much more complex and subtle, as the roles of stakeholders often conflict and are paradoxical.

One such paradox is that governments want to ensure cybersecurity, but at the same they want access to the data of individuals and organizations for surveillance purposes. The whole discussion of 'backdoor' access to data reveals the paradox encountered by governments. On the one hand, governments want companies and citizens to protect themselves, but on the other hand, they do not want them to use encryption and other cybersecurity measures, as this might allow terrorists and criminals to hide their traces. Governments thus often attempt to balance good and evil by allowing encryption, but requiring *backdoors* to remotely access the encrypted devices. Such backdoors can also be exploited by others and merely shift cybersecurity threats from the front door elsewhere. Although it might have its merits, it also further complicates cybersecurity – in particular, its visibility.

Cybersecurity breaches cannot be stopped at a nation's borders. In fact, it is difficult to determine where the actual borders are in cyberspace. Where do governments stop? When are they acting within another nation's territory? What happens when there are attacks from another territory and that country denies involvement? Can one country expect another country to take measures against them? Or can one retaliate on servers located outside one's own country? With borders being hard to define and secure, cybersecurity can become a supranational issue, and perhaps is so by its very nature. The differences between countries can be subtle, as the USA and EU are on the same page with the general direction, but foster different values. Often these are founded in the path dependencies influenced by the history of nations. The 9/11 terror attack had a large influence on the USA cybersecurity policy, whereas the Germany constitution, created after the second World War, ensures the privacy to avoid spying of citizens. The paradox is that to address cybersecurity threat, countries need to collaborate; however, they do not trust each other, as their respective activities and intentions might only be partly visible or do not agree on shared values. Collaboration and conflict are intertwined with each other like espionage and war.

Who are the villains? Hackers range from teenagers, freedom fighters, disgruntled employees, to criminal enterprises or state-sponsored endeavours. The motives of attackers are diverse and not always clear. They might include impressing others, gaining prestige and a reputation, jealousy, revenge, profit-making, political agenda or espionage. Moreover, *who* attacks *what* is not clear, as attacks cannot easily be traced to the hackers or their motives. Attackers might even be insiders; or outsiders might be helped non-intentionally by insiders through unsafe behaviour. Often these activities are masked by normal activities and it is only after damage has occurred that organizations become aware of what was happening. The paradox is that although the impact might be visible, he the attacks and the enemies are hard to determine.

Requirements stipulated by governments might result in significant burdens and costs for companies. Often it is assumed that companies will ensure safety and security for their clients on the internet; however, many companies still ask themselves whether investment in cybersecurity will provide returns in comparison to the cost of a data breach. Data breach costs are associated with resolving the matter, as organizations compensate their clients, pay fines and court fees, invest in forensic and investigation processes, and take counter and preventive measures. Complete protection is never possible and cybersecurity comes at a price.

The reputation of companies and other organizations plays a major role in retaining the trust of clients. Companies do not want to be associated with cybersecurity hacks or viewed as having not taken appropriate security measures. How much do companies spend on cybersecurity? Companies might be reluctant to share information on their cybersecurity spending with the public. The paradox is that too little spending might indicate that they are not well protected, while too much spending might send the message that they are overly concerned – that they might be the potential target of hackers, or simply wasting money. In relation to cybersecurity, it is impossible to take a one-size-fits-all approach to a 'company'. Organizations are diverse and have different demands, a bank and a hospital demand higher levels of security than a restaurant. Moreover, a company's level of knowledge, expertise, experience, their systems, their vulnerability, and the possible impact of a cybersecurity breach are all different. This makes it difficult to talk about companies in general and what is expected from them in cyberspace. How can their security be regulated by governments?

Society is heterogeneous, and as cybersecurity attacks are often not visible, people might not even be aware of them, apart from reports in the media. In addition, most people might not suffer directly from a