TU Delft

Delft University of Technology

Building Cybersecurity Awareness

de Bruijn, Hans; Janssen, Marijn

DOI
10.1016/j.giq.2017.02.007

Publication date
2017

Document Version
Final published version

Published in
Government Information Quarterly: an international journal of information technology management, policies, and practices

Citation (APA)
de Bruijn, H., & Janssen, M. (2017). Building Cybersecurity Awareness: The need for evidence-based framing strategies. Government Information Quarterly: an international journal of information technology management, policies, and practices, 34(1), 1-7. DOI: 10.1016/j.giq.2017.02.007

Important note
To cite this publication, please use the final published version (if applicable).
Please check the document version above.

Copyright
Other than for strictly personal use, it is not permitted to download, forward or distribute the text or part of it, without the consent of the author(s) and/or copyright holder(s), unless the work is under an open content license such as Creative Commons.

Takedown policy
Please contact us and provide details if you believe this document breaches copyrights.
We will remove access to the work immediately and investigate your claim.

This work is downloaded from Delft University of Technology.
For technical reasons the number of authors shown on this cover page is limited to a maximum of 10.

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.

© 2017 The Author(s). Published by Elsevier Inc. This is an open access article under the CC BY-NC-ND license (http://creativecommons.org/licenses/by-nc-nd/4.0/).

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
0740-624X/© 2017 The Author(s). Published by Elsevier Inc. This is an open access article under the CC BY-NC-ND license (http://creativecommons.org/licenses/by-nc-nd/4.0/).

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

cyberattack. Banks, credit card companies and shops might take the risks themselves and in this way protect society. The paradox is that while organizations do not benefit from making the problems and attacks visible, this visibility is necessary to create a greater sense of urgency and initiate action.

For citizens, the interconnectivity and data generated by devices has resulted in 'an unprecedented improvement in the quality of life' (Elmaghraby & Losavio, 2014, p. 491). At the same time, the vast amount of data available about citizens' location, activities and even emotions, is giving rise to cybersecurity and privacy challenges. The paradox here is that the same data that can be used to improve the quality of life can also be used against citizens. Data-sharing introduces a vulnerability that can be exploited by hackers. Stolen data might be used to blackmail someone, the public availability of health data of an individual might result in difficulties obtaining a mortgage or having to pay higher insurance premiums. Moreover, potential targets might be selected based on the data accessed; for example, sending fake messages with instructions for payment into a bank account based on buying behaviour; or phishing, resulting in the installation of malware, which takes control of a system/computer, such that the user cannot access the system unless they pay a ransom (in Bitcoins to avoid traceability).

Cybersecurity is a necessity and the question is even if systems connected to the Internet should be even sold without ongoing cybersecurity protection. Why de governments not require the proper protection of systems that are sold by law? Companies and citizens who have spent money on cybersecurity and have monitoring software, firewalls, secure authentication, for example, might also still ask whether their security is working. Would they have been hacked if they had not taken precautions? Is there any return on the investment? You only really understand the importance of security when you do not have it and something happens. Responsibilities are not clear and fragmented among stakeholders. The paradox is that those who can or should provide security might not suffer from the consequences, and can avoid the taking of responsibility. This results in limited urgency to act and no direct need to invest to protect the cyberphysical society.

Despite the risks, people are often not worried about cybersecurity. They have often not experienced any impact and are not interested. Cybersecurity is like infrastructure – you take it for granted and only realize its importance when you experience a problem, but then it is too late. Cybersecurity can also be viewed as a quasi-public good (common good) that nobody owns but everybody is involved in and can be affected. This makes it difficult to pinpoint who should be responsible in taking action and ensuring safety and security.

Who is to blame for all these threats? Are the companies who provide potentially vulnerable software responsible for damages? Are companies that trade without having high levels of cybersecurity in place acting responsibly? Or should we blame individual staff who were aware that their actions might be harmful, or individual citizens who did not sufficiently protect their systems? Or is a government that does not provide appropriate security to its constituents ultimately responsible?

Paradoxes complicate the communication and framing of cybersecurity as the other end of the contradiction can be used as a counterargument. An overview of the paradoxes and underlying policy questions is presented in Table 1. Raising political awareness in such a sea of paradoxes is not easy. Politicians must demonstrate to their constituencies that they are in control, but if nothing happens, public interest and the sense of urgency in relation to cybersecurity will decrease. Politicians would like to ensure the issues remain visible to citizens, but this is difficult. Often cybersecurity is viewed primarily as a technical challenge: as long as it is organized properly and an appropriate budget is allocated nothing else needs to be done. In practice, the issues are not so straightforward, there are no clear responsibilities, boundaries are difficult to define, and the required level of security is also difficult to determine. In addition, the types of measures needed and the level of risk taken are unclear, as is the question of who needs to be protected. Last but not least, people may not be aware that their behaviour could be harmful or that they could become under attack.

Table 1
Overview of policy-making paradoxes.

Policy-making question	Description of the paradox
What is the desired level of protection of systems?	Governments want companies and citizens to protect themselves. Nevertheless, government want to have a backdoor to control and detect criminality and terrorism.
How much (cross-border) collaboration is necessary to fight cybersecurity?	Countries need to collaborate as cybersecurity is a global phenomenon, however, they do not trust each other as they might be active in hacking each other.
Who to fight to?	Despite that impact of attacks are often visible, the attacks and villains are hard to determine.
What is the right amount of spending on cybersecurity?	Too little spending on cybersecurity might indicate that they are not well protected, while too much spending might send the message that they are overly concerned and there might be something wrong.
What is the right level of visibility?	Organizations do not benefit from making the problems and attacks visible to their customers as they might decrease faith and trust. Yet, this visibility is necessary to create a greater sense of urgency and initiate action.
How will the data be used?	The same data that can be used to improve the quality of life can also be used against citizens.
Who should ensure the cybersecurity of systems?	Organizations providing or who can provide security might not suffer from its impact.

3. Why is cybersecurity policymaking so challenging?

The overview of stakeholders, their various roles, attitudes and behaviour has demonstrated the many paradoxes involved in a complex ecosystem in a cyberphyscial society. Ignorance, a limited understanding of what needs to be done, limited awareness of the issue despite its significance and urgency, have resulted in a lack of action, planning and policies. What makes communication in this area so challenging? Below, we discuss four reasons why it is difficult for policymakers.

3.1. Intangible nature

When people feel pain they become aware that something is not right. In the same way, often the public only becomes aware of a problem after they experience its impact. The impact of cybersecurity breaches is often not visible in a physical sense, or the precise consequences might not be tangible at all; for example, in the recent US elections, it appears that the Democratic Party was hacked, but the real effect remains unclear (Lipton, Sanger, & Shane, 2016). Moreover, there might be an impact, but not one that is visible, as in the case when financial institutions are required to compensate the victims of online fraud. These financial institutions do not benefit from making these breaches visible, as it might undermine trust in their operation. Consequently, the impact remains largely invisible and intangible to those not directly affected.

Cybersecurity is thus largely invisible to the public. There are no cameras capturing images of military vehicles and combatants, as occurs in regular wars. How can cybersecurity breaches be visualized? Often experts investigate traces of attacks and visualize them on a map, which reveals what is going on and the instruments employed by hackers. What do those maps show? Collecting 'hard' evidence is difficult, and uncertainty remains about the possible victims, the location of the hackers and their motives.

Cybersecurity is often not easy to explain, as there are many aspects. Hackers have the ability to move from one server to another to cover their path and origins. Without extensive effort it is often difficult to find those who carried out an attack. Moreover, even if the initiating computer can be found, this does not mean that the owner carried out the attack. Hackers and security specialists are in a continuous battle to outsmart each other, while politicians must depend on their intelligence agencies and deal with the uncertainties of their analyses.

3.2. Socio-technical dependence

Cybersecurity concerns both humans and systems, but the complexity of this interaction goes beyond the understanding of most people. Deep knowledge of cybersecurity, of IT infrastructure and the types of attacks that are possible are necessary to understand what is going on. However, it is not merely technology that plays a role. It has often been stated that humans are the weakest link in the cybersecurity chain. Humans play a role in maintaining and updating systems to ensure that the newest defences are in place, that attacks are detected immediately, and countermeasures can be taken. This also requires policies to be in place and that people understand what is required, as we know that unawareness on the part of users can introduce further vulnerabilities; for example, by using weak passwords, installing untrustworthy software and using insecure devices and applications.

The socio-technical nature of cybersecurity thus complicates the process of finding solutions. In contrast to global warming and climate change, where a polluting energy plant can be replaced by a low carbon emissions plant, there are no straightforward solutions in the field of cybersecurity. People want to be safe and secure, but may not want – or simply do not have the money – to take action. The public expects that the government will take responsibility, but the measures implemented by governments might not be sufficient if individuals do not also take some responsibility.

3.3. Ambiguous impact

It is difficult to judge cybersecurity risks in advance. What impact will there be if data is stolen or altered? Often no physical systems are damaged or money stolen, although there are exceptions, such as the Stuxnet virus in Iran, in which centrifuges were damaged (Langner, 2011).

Most people perceive possible risks as remote. Who the hackers will target next is not known, and organizations and individuals tend to think that they will not be the target of an attack – it might happen to my neighbour or another company, but it will not happen to me. Moreover, when it does happen to someone else, others often think it was their own fault, and that they probably failed to take necessary security measures. This is a fallacy, as despite all their good intentions and countermeasures, there is always the potential that an organization will suffer a cybersecurity attack.

Furthermore, if most people fail to acknowledge that cybersecurity is a problem, the tendency will be to ignore it and fail to take appropriate action. The lack of a sense of urgency in many people results in no common action.

Cybersecurity entails a continuous battle, with both the attackers and those who are protecting us against them remaining constantly on the move. The impact of new attacks and technologies is unclear, as are the defence requirements. What resources are required to fight the unknown? Cybersecurity is never completely guaranteed, which makes it difficult to demonstrate the successes and call for investment. What is the return on investment in cybersecurity measures? This is further complicated, as despite all the best efforts there might always be a risk of cybersecurity violations, and this is a difficult message to convey. Whatever you do, might not be sufficient.

3.4. Contested nature of fighting cybersecurity

Once the urgent need for cybersecurity has been established, a discussion about the measures that need to be taken is required. Organizations are often uncertain about the measures that need to be taken to improve security. Attackers are often anonymous and it is unclear who the enemy is.

Everybody can be a potential enemy. Even friendly servers or the computers of employees might be hacked and become a threat. To fight cybersecurity, network traffic needs to be monitored, but the human behaviour of both friends and enemies can also be tracked. In other words, monitoring comes at the expense of the privacy of individuals. Ensuring cybersecurity thus comes at the cost of other public values, and these measures are contested.

Some argue that cybersecurity is not always for the good. Discussion about the NSA is dominated by privacy issues and its ability to act without oversight from elected politicians or any institutional accountability. The development of surveillance programmes should strike a better balance between security and privacy (Reddick, Chatfield, & Jaramillo, 2015). Moreover, the wording used to frame a problem can have effects, from mobilizing resistance to greater attention being paid to the issue (De Bruijn, 2014).

There is an acknowledged tension between national security and civil rights (Gorham-Oscilowski & Jaeger, 2008), with citizens contesting NSA surveillance programmes and their needs. These findings suggest that governments need to be more efficacious and more transparent in communicating about surveillance programmes if they are to gain greater approval for such programmes (Reddick et al., 2015).

In summary, there is growing concern about the ways in which our lives are increasingly regulated and controlled, whether in relation to ordinary objects or technology (Woolgar & Neyland, 2013). Can the privacy of employees and citizens be sacrificed for the sake of cybersecurity? Do the advantages outweigh the disadvantages?

4. Why do we need framing?

The challenges discussed in the previous section mean that politicians and policymakers face a difficult task. How do we fight an unknown enemy or someone who denies responsibility in a situation where it is hard to prove that they are the culprit? Also researchers are challenged to frame the outcome of their research in a concise way without Message framing is aimed at communicating a complex problem in a simple and convincing manner.

Cybersecurity specialists often attempt to use message framing, but often fail to get the right message across. They use management guru techniques and manipulate common cognitive vulnerabilities in order to over-dramatize and over-simplify cybersecurity risks (Quigley, Burns, & Stallard, 2015). This does not result in the attention desired: critical systems remain unprotected and behaviour does not change or cybersecurity protection is delegated to software and hardware providers including automatic update measures, resulting in people feel cyber-secure and stop paying attention. Instead, the public might recognize the over-dramatization or consider the issue too difficult to deal with, resulting in inertia. Why do these frames not work? One reason is that there is no clear victim and no visible enemy. While the identification of a hero and a villain is commonly used in framing to create a convincing message (De Bruijn, 2017), framing cybersecurity in this way does not result in the desired attention and sense of urgency.

Cybersecurity can be perceived as a problem of the individual or as a problem of society. Presenting it as a collective problem to be tackled by society is difficult for politicians and policymakers, as they do not have much to gain by addressing this topic, the effects of which are largely invisible to the public. All politicians agree that cybersecurity is important and view it as a technological issue that needs to be resolved. Generally speaking, it is a bipartisan issue that they cannot use to differentiate themselves from their political opponents. Nevertheless, the four

challenges mentioned above demonstrate that cybersecurity is more than merely a technological problem and that political values are involved.

The problem contexts that define and shape practice are considerably more complex than can be easily explained and captured in a simple frame. Framing requires comprehensive analysis and deep understanding of the context (see Janowski, 2015). This complexity, the uncertainties and multifaceted challenges in cybersecurity means it is difficult to create a simple frame.

5. What is message framing?

Message framing is a strategy for communicating a complex problem in such a way that the main arguments are understood and cannot be easily challenged (De Bruijn, 2017). The characteristics of the source of information as well as of the recipient may influence both the direct and indirect effects (De Vries, 2017). The effect of message framing on decision-making and persuasion has been well researched (Smith & Petty, 1996). One approach that has been used to understand the effects of framing is known as 'prospect theory' (Kahneman & Tversky, 1979). This theory states that people evaluate information in terms of either potential gains (positive framing) or potential losses (negative framing). Preferences can be altered by changing the way information is presented. How people's attitudes and behaviour are affected by message framing is dependent on the processing and traits of the receiving party. For example, Maheswaran and Meyers-Levy (1990) found that positively framed messages are more persuasive when the receiver does not read the message in detail, whereas negatively framed messages are more persuasive when detailed processing is emphasized. Furthermore, the context in which a message is framed also determines its effectiveness (Rothman & Salovey, 1997). De Vries, Terwel, and Ellemers (2014) use experiments to show that adding irrelevant information dilutes the impact of highly relevant information.

Message framing requires reducing the complexity to clear and easy to explain messages. As we have seen, cybersecurity is a complex socio-technical phenomenon involving many facets. Attempting to communicate this complexity results in an incomprehensible and unclear story that takes too long to communicate. The essence of message framing is to develop a relatively simple framing of a complex reality: the complexity has to be reduced to a relatively simple message capturing the essence. The reduction of complexity is by definition a debatable solution, as relevant issues might be omitted (De Bruijn, 2017).

Typically, framing positively and negatively results in valence framing effects (Kahneman & Tversky, 1979). This is called the risky choice framework, which reveals the consequences of action or inaction (Levin et al., 1998). In such a strategy, both utopian and dystopian views are presented, creating the desire for action by showing what will happen if no action is taken (dystopian view) or what the result of taking action might be (utopian view). In these frames, people are more likely to take risks when attention is focused on the opportunity to avoid losses than when the focus is on the opportunity to realize gains (Kahneman & Tversky, 1979; Levin et al., 1998): the 'typical pattern is a choice reversal or a choice shift in the direction of less willingness to take a risk when the choices are framed positively than when choices are framed negatively' (Levin et al., 1998, p. 153). Levin et al. (1998) identified three types of frames:

1. The standard risky choice framing – which influences the valences in terms of willingness to take a risk.
2. Attribute framing – which affects the evaluation of object or event characteristics.
3. Goal framing – which influences the persuasiveness of a communication.

Embracing an utopian view can result in the a *boomerang effect* (De Vries, 2017). De Vries demonstrates in which positively framed communication about low-carbon technologies result in the perception of being manipulated and may actually lead to opposition in the long run.

De Bruijn (2017) used the Victim-Villain-Hero (VVH) model to understand framing, identifying five criteria of successful frames:

- Frames are catchy
- We intuitively agree with frames
- Frames contain a villain
- Frames challenge your opponent's core values
- Frames tap into social undercurrents

All these approaches remain at a relatively theoretical level and provide limited guidance on how to frame an actual situation. Therefore, we will derive some more specific framing strategies below. While framing is about conveying the message, *evidence-based* policymaking is about ensuring that it is factual and appropriate data is collected. We argue that although one could view these as conflicting, they should be viewed as complementary. The same evidence can be framed in a different way, resulting in valence framing effects.

Cybersecurity policy-makers, specialist and scientist are often criticized for not being able to explain their message to the public. Although they have the evidence, they are not always able to convey the message to the public and convince politicians and policymakers to take action. A typical example is environmental science, with scientists unable to convince policymakers of the urgency to reduce carbon emissions (De Vries et al., 2014). What is required to address this failure is *evidence-based message framing*.

6. Evidence-based message framing strategies

The concept of 'evidence-based framing' has two implications. First, it means that frames should be based upon facts. Messages that are, for example, purely emotional will not live long, as they are subject to public scrutiny. People will find out that the message is not correct and will start distrusting the messenger. Regaining trust once it is lost takes much more effort or might even be impossible. Messages should thus be grounded in evidence that is collected in such a way that it can be trusted. Second, facts need good frames. Climate scientists have been criticized for not effectively explaining their message to the public – they were unable to frame their message properly (Crompton, 2010). Therefore, there is a need for *evidence-based message framing*.

In this section, we propose a series of strategies which frame cybersecurity in such a way that more societal and political awareness will be generated. We base our strategies on both the more generic literature

Table 2
Summary of framing strategies.

Strategy	Description of an effective frame
1) Do not exacerbate Cybersecurity	Put the need in a realistic perspective. Exaggeration will only exacerbate the problem and work against the objective in the long term.
2) Make it clear who the villains are	Villains should be clearly recognizable as evil.
3) Give cybersecurity a face by putting the heroes in the spotlight	Those who are guarding and protecting society should be placed in the forefront. Demonstrate their successes.
4) Show its importance for society	The benefits of taking action should be emphasized. Cybersecurity is key to economic growth and the prosperity of nations.
5) Personalize for easy recognition by the public	Connect cybersecurity to the daily life of people to ensure easy recognition. Groups are different.
6) Connect to undercurrent	Cybersecurity is closely interwoven with other issues that do receive political attention.

on framing, and on empirical research on framing in the specific area of global warming. Table 2 provides an overview of the strategies.

6.1. Do not exacerbate Cybersecurity

There is a dystopian view of cybersecurity, in which cybercrime is seen as a potential threat everywhere: when you pay for something using a card; when you change the temperature in your living room; when you are driving or walking along the street (cameras are watching you). Some argue that cybercrime will have a devastating impact on our lives: there will be no more privacy, and a big brother society will emerge. In such a society, you will never be safe and the risks will be immense.

The problem with this dystopian way of framing cybersecurity can be summarized in the well-known one-liner: '*Hell does not sell*'. This is a lesson learned from discourse on the issue of global warming. Overdramatizing the impact of global warming ('catastrophic', 'fast', 'irreversible') results in a mixture of denial, apathy and fatalism (O'Neill & Nicholson-Cole, 2009). It also feeds the idea that we are out of control – that the problem can no longer be resolved. The same risk applies in relation to cybersecurity. What impact does the message that you are never safe and the risks are immense actually have on people? Instead of creating a sense of urgency, it might result in denial.

There is another lesson we can learn from the debate about global warming. Once people are in a mood of denial and apathy, they become very receptive to the message that human-made global warming simply does not exist – that it is a hoax. The same could happen in relation to cybersecurity if the risks are over-dramatized. For example, billions were spent on the millennium bug, but nothing disastrous happened. The argument might be made that the threat is not as bad as advocated by the experts.

6.2. Make it clear who the villains are

The problem with framing cybersecurity is that there are often no clear villains: the villains may not visible; the victims may also be villains; the victims might have an interest in not being explicit about the villain; or the presumed villain might be perceived as a hero – as might be the case with hackers. The activist group "Anonymous" might be viewed as a villain or as a hero, dependent on your point of view. The DDoS attack to the Canadian government websites in 2015 after passing the terrorist bill can be viewed as trying to safe privacy of people, but also as an act of terrorism.

The absence of a clear villain makes it harder to frame cybersecurity in an effective way. The implication of this observation is clear: give the villain a face. Provide clear examples of unambiguous villains – cyber gangs that are, without doubt, perpetrating extreme acts. Be explicit about their strategies – how they can ruin the lives of their victims. These villains will of course not represent the whole family of unambiguous and ambiguous villains, but this is not the issue. The issue is that without a clear and unambiguous villain, framing cybersecurity will remain problematic. If there is a clear villain, there will be obvious victims. This helps people to more easily identify with the fight against cybercrime.

Thus, villains need to be clearly recognizable. Such a villain could be a country with already have been the villain in other areas or Nigerians who are notorious for their scam emails. However, only cast unambiguous cybercriminals as the villains. Casting a young hacker as the villain may result in 'sympathy for the enemy' and have an inverse effect.

6.3. Give the fight against cybersecurity a face: put the heroes in the spotlight

Giving villains a face is important – but the same goes for the heroes. The heroes are those who are protecting us, those whose expertise and dedication we rely on. For most people, our cybersecurity heroes do not have a face. Who are they? Is it possible to meet them? Most people have no clue about the people who are protecting us: Are there special departments of smart people located in basements, or computer nerds sitting in attics? Heroes might be hard to find, and heroes might not look heroic at all.

By making these dedicated people working on our safety and security visible, we gain a better understanding of who is guarding and protecting society. This is a framing strategy that is sometimes used in relation to large infrastructure projects that have the potential to harm the interests of residents or other stakeholders; for example, because they take a lot of time. Giving the people who work on a project a face, a hard working person with a helmet. Reveal the complexity of their work and making explicit the high level of their professionalism might be conducive to a respect for their knowledge and acceptance of their work by others. By giving the 'cyber heroes' a face and revealing what they do, it becomes clear that they are undertaking extremely complex work to keep our systems secure. Select a smart young guy with a degree or a renowned university and make the person visible in the news and at late night shows. They might be the smartest in their class and come from all over the world. If we recognize their expertise and experience, we gain confidence that they are doing a good job. By bringing them to the forefront people can recognize their work and see how their work is done. The public can identify themselves with the 'heroes' and their work and thus with the fight against cybercrime. This can all be further strengthened by also demonstrating the successes of their work: often only failures make the news, while the successes remain invisible.

6.4. Connect cybersecurity to values other than security alone

In relation to environmental policy in general and global warming in particular, connecting to other values is a well-known framing strategy (De Bruijn, 2017). In order to convince right-wing opponents of the need for environmental policies, for example, these policies are linked to right-wing values, such as strengthening the economy and entrepreneurship. It is argued, for example, that investing in sustainability is good for the economy, will bring jobs and innovation. The idea is that linking a policy to other people's values might make them more receptive to this policy (De Bruijn, 2017).

The same strategy could be applied to the framing of cybersecurity. Investing in cybersecurity could bring economic benefits – not so much because there will be fewer costs of crime, but because countries investing in fighting cybercrime will build up expertise that is of high value. This might strengthen the IT industry, it might make a country a key player in the cybersecurity domain, with the nation becoming an international frontrunner, resulting in the creation of new jobs and the exporting of knowledge. Cybersecurity need not be framed solely as a task of solving problems, but also as creating economic opportunities – which might make it attractive to invest in expertise in cybercrime.

6.5. Personalize for easy recognition

Society is not homogenous and people have different interests and levels of knowledge and experience. It is crucial to understand that there are multiple audiences (individuals, businesses, nations, societies) which require different messages. Personalization of the message is an important framing strategy, which should ensure that the problem is recognizable in daily life.

If complex and abstract topics such as cybersecurity are made relevant to people's immediate living environment, then they will readily recognize the urgent need to address cybersecurity. For example, companies in high-tech industry will be more receptive to threats of espionage and the risk of their ideas being stolen and used by other organizations, while citizens will better understand the need when faced with the possibility of stolen or blocked credit cards and the risk

of losing money. Both groups also require different instruments to ensure their safety in cyberspace.

6.6. Connect to other tangible and clear issues

Finally, there are always issues that stimulate people much more than cybersecurity, but that are also interwoven with cybersecurity. This is because these other issues are highly visible and have gained some momentum. As such, they can be used to gather support for the fight against cybercrime. The most powerful example is the threat of IS (Islamic State), which can be used to strengthen the argument for cybersecurity. We can emphasize the importance of cybersecurity to deal with the threat of IS, as it relies on the internet to plan terrorist activities: cybersecurity can help in detecting and preventing these. Moreover, their financial resources and plans should be monitored – and we need 'cyber heroes' for that.

7. Conclusions

Our society is turning into a cyberphysical society having dependence on Information and Communication Technology (ICT) across all aspects of our daily lives, which makes the need for cybersecurity paramount. The intangible nature of cybersecurity, the socio-technical dependences, the ambiguous impact and contested nature of fighting cybersecurity all make it a challenging area for policymakers. Cybersecurity can be framed in different ways, having different effects on people. Cybersecurity is a complex and multifaceted area which has no clear heroes or villains. The inability to frame cybersecurity has resulted in a failure to take appropriate measures and develop suitable policies. However, there are already ongoing cyberwars, and citizens and governments need to be better prepared. Message framing is a strategy for communicating a complex problem in such a way that the main arguments are understood and cannot be easily challenged. Simple message frames do not work for cybersecurity and therefore *evidence-based message framing* is necessary. In a similar vein to evidence-based policymaking, messages are framed based on the evidence and use framing strategies. Thinking in terms of framing strategies to communicate a difficult message has profound implications. We argue that it is important to take the evidence as a starting point and avoid utopian and dystopian frames, as these standard messaging strategies might be counterproductive. Instead, the following six strategies were identified as offering a better way to frame cybersecurity: 1) do not exacerbate cybersecurity, 2) make it clear who the villains are, 3) give cybersecurity a face by putting the heroes in the spotlight, 4) connect cybersecurity to values other than security alone, 5) personalize the message for easy recognition and 6) connect to other tangible and clear issues.

Message framing is not only important or cybersecurity but in many domains of government information. For example, the discussion about privacy, the use of personal files, identify management, Internet governance, public-private systems, and the opening of data are all complex socio-technical areas in which the results of intensive research are not easily to communicate. Cybersecurity specialists and experts, but also researchers and policy-makers, needs to frame their message well to avoid misunderstanding and ambiguity. Capacity building by government and more research about evidence-based framing strategies and its effectiveness is needed.

Acknowledgement

The authors would like to thank Tomasz Janowski for arranging the reviews and his suggestions.

References

Arora, A., Nandkumar, A., & Telang, R. (2006). Does information security attack frequency increase with vulnerability disclosure? An empirical analysis. *Information Systems Frontiers, 8*(5), 350–362.
Crompton, T. (2010). *Common cause: The case for working with our cultural values.* WWF, Oxfam, Friends of the Earth, CPRE, Climate Outreach Information Network.
De Bruijn, H. (2014). *Framing. Over de macht van taal in de politiek.* Amsterdam: Atlas Contact.
De Bruijn, H. (2017). *The art of framing: How politicians convince us that they are right.* Etopia BV.
De Vries, G. (2017). How Positive Framing May Fuel Opposition to Low-Carbon Technologies: The Boomerang Model. *Journal of Language and Social Psychology, 36*(1), 28–44.
De Vries, G., Terwel, B. W., & Ellemers, N. (2014). Spare the details, share the relevance: The dilution effect in communications about carbon dioxide capture and storage. *Journal of Environmental Psychology, 38*, 116–123. http://dx.doi.org/10.1016/j.jenvp.2014.01.003.
Doty, P. (2015). U.S. homeland security and risk assessment. *Government Information Quarterly, 32*(3), 342–352. http://dx.doi.org/10.1016/j.giq.2015.04.008.
Elmaghraby, A. S., & Losavio, M. M. (2014). Cyber security challenges in smart cities: Safety, security and privacy. *Journal of Advanced Research, 5*(4), 491–497.
Gorham-Oscilowski, U., & Jaeger, P. T. (2008). National Security Letters, the USA PATRIOT Act, and the Constitution: The tensions between national security and civil rights. *Government Information Quarterly, 25*(4), 625–644. http://dx.doi.org/10.1016/j.giq.2008.02.001.
Hernández-Ramos, J. L., Jara, A. J., Marın, L., & Skarmeta, A. F. (2013). Distributed capability-based access control for the internet of things. *Journal of Internet Services and Information Security (JISIS), 3*(3/4), 1–16.
Janowski, T. (2015). Digital government evolution: From transformation to contextualization. *Government Information Quarterly, 32*(3), 221–236. http://dx.doi.org/10.1016/j.giq.2015.07.001.
Kahneman, D., & Tversky, A. (1979). Prospect Theory: An analysis of decisions under risk. *Econometrica, 4*, 362–377.
Langner, R. (2011). Stuxnet: Dissecting a cyberwarfare weapon. *IEEE Security and Privacy, 9*(3), 49–51.
Leuprecht, C., Skillicorn, D. B., & Tait, V. E. (2016). Beyond the Castle Model of cyber-risk and cyber-security. *Government Information Quarterly, 33*(2), 250–257. http://dx.doi.org/10.1016/j.giq.2016.01.012.
Levin, I. P., Schneider, S. L., & Gaeth, G. J. (1998). All frames are not created equal: A typology and critical analysis of framing effects. *Organizational Behavior and Human Decision Processes, 76*(2), 149–188.
Lipton, E., Sanger, D. E., & Shane, S. (2016, 13 December). *The Perfect Weapon: How Russian Cyberpower invaded the U.S.* The New York Times.
Maheswaran, D., & Meyers-Levy, J. (1990). The Influence of Message Framing and Issue Involvement. *Journal of Marketing Research, 27*(3), 361–367. http://dx.doi.org/10.2307/3172593.
O'Neill, S., & Nicholson-Cole, S. (2009). 'Fear Won't Do It'. Promoting Positive Engagement With Climate Change Through Visual and Iconic Representations'. *Science Communication, 30*(3), 355–379.
Quigley, K., Burns, C., & Stallard, K. (2015). 'Cyber Gurus': A rhetorical analysis of the language of cybersecurity specialists and the implications for security policy and critical infrastructure protection. *Government Information Quarterly, 32*, 108–117. http://dx.doi.org/10.1016/j.giq.2015.02.001.
Reddick, C. G., Chatfield, A. T., & Jaramillo, P. A. (2015). Public opinion on National Security Agency surveillance programs: A multi-method approach. *Government Information Quarterly, 32*(2), 129–141. http://dx.doi.org/10.1016/j.giq.2015.01.003.
Rothman, A. J., & Salovey, P. (1997). Shaping perceptions to motivate healthy behavior: The role of message framing. *Psychological Bulletin, 121*(1), 3–19. http://dx.doi.org/10.1037/0033-2909.121.1.3.
Smith, S. M., & Petty, R. E. (1996). Message framing and persuasion: A message processing analysis. *Personality and Social Psychology Bulletin, 22*, 257–268.
Ten, C. W., Liu, C. C., & Manimaran, G. (2008). Vulnerability Assessment of Cybersecurity for SCADA Systems. *IEEE Transactions on Power Systems, 23*(4), 1836–1846. http://dx.doi.org/10.1109/TPWRS.2008.2002298.
Woolgar, S., & Neyland, D. (2013). *Mundane Governance: Ontology and Accountability.* Oxford University Press.
Zhao, J. J., Zhao, S. Y., & Zhao, S. Y. (2010). Opportunities and threats: A security assessment of state e-government websites. *Government Information Quarterly, 27*(1), 49–56. http://dx.doi.org/10.1016/j.giq.2009.07.004.