SOURCE | Societal Security Network

VIRTUAL CENTRE OF EXCELLENCE FOR RESEARCH SUPPORT AND COORDINATION ON SOCIETAL SECURITY

REPORT

WORKSHOP 'PREPAREDNESS FOR CYBERSECURITY'

29 NOVEMBER 2018, THE HAGUE

This project has received funding from the European Union's Seventh Framework Programme for research, technological development and demonstration under grant agreement no 313288.

Contents

Goals and focus of the workshop

The goal of this workshop is to discuss possible measures to improve *preparedness* for cybersecurity.

The workshop focused on exploring *values that are at stake in the design and implementation of such measure,* and possible conflicts between such values. For example, on the one hand the values that are implicit in the design and implementation of security measures ('industrial values'), and on the other hand the values held by citizens and other beneficiaries of these measures ('societal values')—and to find ways to (better) harmonize these sets of values.

The workshop lasted two-hours. Participants were several experts on cybersecurity, from the Dutch Ministry of Justice and Security, Delft University of Technology, The Hague University of Applied Sciences, and TNO. They were already familiar with the (Dutch) Nederlandse Cybersecurity Agenda and the (Dutch) National Cyber Security Research Agenda III NCSRA. In the workshop we explored and discussed a range of ideas for creating measures to improve preparedness for cybersecurity.

Below are initial thoughts on ***preparedness*** and on ***values***—which were input for the workshop.

Focus on preparedness

In order to provide focus to the workshop, we will focus on preparedness—one of the phases or activities that we can distinguish in cybersecurity:

- Prevention: what one can do in order to prevent cyberattacks, e.g., combat cyber-criminality or measures that decrease the chances of cyberattacks;
- **Preparedness: what one can do to be better prepared against cyberattacks, e.g., measures to better sustain a cyberattack, reduce the damage, or to keep things going as much as possible;**
- Crisis management: what one can do during a cyberattack, e.g., to reduce the damage—apart from what is already done through prevention and preparation;
- Repair: what one can do after a cyberattack, to bounce back, to repair damage, possibly even to be better able to withstand cyberattacks a next time.

We propose to focus on preparedness, partly because it is sometimes relatively underdeveloped, and partly because it raises many questions: How much do we want to invest in preparedness? How to balance priorities for preparedness, in comparison to, e.g., prevention, crisis management and repair? Who should be responsible—the state, specific agencies, or citizens? Please note that the concept of preparedness has overlaps with the concept of resilience (https://ec.europa.eu/digital-single-market/en/news/resilience-deterrence-and-defence-building-strong-cybersecurity-europe).

We can draw parallels to preparedness in other domains, e.g., preparedness for flooding or for a nuclear incident. The Dutch government advises (https://crisis.nl/wees-voorbereid/tips/): to have an emergency kit ready (radio on batteries; torch; spare batteries; first aid kit; matches, in waterproof packaging; small candles; blankets; tools; and an alarm whistle); to be informed about specific risks, depending on where you live; to know what to do when the sirens sound; etc. And they have specific

advice for, e.g., flooding (https://crisis.nl/wees-voorbereid/overstroming/) or nuclear incidents (https://crisis.nl/wees-voorbereid/stralingsincident/). Also for cyber attacks (https://crisis.nl/wees-voorbereid/cyberaanval/): to update software; to use anti-virus software; to use passwords wisely; to make backups frequently; to only connect to trusted networks (not, e.g., in bars); etc.

Focus on values

We expect that different stakeholders will have different values regarding cybersecurity and preparedness, and that these values will need to be made explicit, negotiated and combined or balanced, during the design and implementation of measures to improve, e.g., preparedness.

In order to guide the discussion, we will look at cybersecurity through the lens of *societal security*: "the ability of a society to persist in its essential character under changing conditions and possible or actual threats" (more info on: https://en.wikipedia.org/wiki/Societal_security).

- A *societal security* lens acknowledges that attacks can come from a wide range of sources and can be aimed at a wide range of targets—attacks do not only happen between one state and another state. This is indeed the case for cybersecurity, where sources can be anything, ranging from a state, non-state groups to criminals, and targets can be anything, ranging from individual citizens, businesses to infrastructure.
- Furthermore, a *societal security* lens views security as a *social* phenomenon—in addition to viewing it as technological (e.g., building specific defensive or offensive capabilities) and economic (e.g., when a state spends public money, or when a company makes money, delivering security products or services). Security as a social phenomenon stresses the viewpoint of citizens, of living collectively and organizing society.

This focus concurs with two shifts that were (briefly) discussed in the NCSRA III: "… a shift ... from disruption for *economic* profit to disruption to *influence societal values and fundamental rights*" (NCSRA III, p. 5); and a shift to "the *humanist and behavioural* side of cybersecurity (NCSRA III, p. 4).

Interestingly, the internet was *not* designed with values like security and protection in mind (although its first version was funded by the US Defence Agency), but with values like freedom and openness in mind (reflecting, e.g., the spirit of academia)[1]. This means that we now have built an internet without some of the security measures that we would like to have now.

Furthermore, we can zoom-in on specific values and tensions between values. We expect, e.g., conflicts between values such as usability and security, accessibility and security, and privacy and convenience (CANVAS White Paper 1: Cybersecurity and ethics). In addition, we can zoom-in on values of different stakeholders. It is possible, e.g., that national politicians will stress short-term success and reacting to incidents; companies will stress implementation and making a profit; citizens will stress

[1] Dunn Cavelty (2014): Breaking the Cyber-Security Dilemma: Aligning Security Needs and Removing Vulnerabilities. *Science and Engineering Ethics*, 20 (3), 701–715.

(subjective perceptions of) privacy, safety and practical usability; local politicians maybe social cohesion; and civil society organizations may stress privacy, equality and democracy.

We took two **values** from the *Charter of Fundamental Rights of the European Union* as focus points: freedom and equality (the other values are, of course, also critical in general, but less immediately relevant for our current purpose:

1. Dignity: right to life and prohibits torture, slavery, the death penalty, eugenic practices and human cloning
2. **Freedoms**: liberty, personal integrity, privacy, protection of personal data, marriage, thought, religion, expression, assembly, education, work, property and asylum
3. **Equality**: equality before the law, prohibition of all discrimination incl. on basis of disability, age and sexual orientation, cultural, religious and linguistic diversity, the rights of children and the elderly. While it stops short of guaranteeing economic rights, the Charter recognises and respects access to services of general economic interest, involving an element of economic equality.
4. Social protection: covers social and workers' rights including the right to fair working conditions, protection against unjustified dismissal, and access to health care, social and housing assistance
5. Citizen's rights: rights to vote in elections and moving freely in accordance with international law.
6. Justice: the right to an effective remedy, a fair trial, to the presumption of innocence, the principle of legality, non-retrospectivity and double jeopardy.

In addition, there are **criteria** for evaluating specific measures for cybersecurity preparedness[2]:

a) **Legality**: Is this cybersecurity measure legal and properly proscribed by law? Does it meet the criterion of subsidiarity (of being implemented at the most local level possible)?
b) **Legitimate Aim**: does the cybersecurity measure pursue a legitimate aim?
c) **Necessity and proportionality**: is the measure necessary and proportionate in a "democratic society"? Can it be achieved in a lower impact or less intrusive way?
d) **Effectiveness**: Can we expect this measure to achieve the aim being pursued? How will impact and effectiveness be measured?
e) **Transparency**: Can this measure be made transparent; can it be explained to others?
f) **Public oversight**: Are there effective and efficient mechanisms for oversight of this measure?
g) **Inclusion, participation**: Can putative users or potential beneficiaries of these measures be involved in the design and implementation of these measures?

[2] Based on principles for 'just war' (Legitimacy; Rights-based approach; Democratic oversight and review; Cohesive; Transparency; Subsidiarity; Civilian, non-military), and dimensions of Responsible Research and Innovation (Owen et al. 2013: Anticipatory; Reflective; Deliberative; Responsive).

Background for the discussion

In order to focus the discussion in the workshop, we used elements from two documents as background: We focused on three (of a total of six) goals of the Nederlandse Cybersecurity Agenda (https://www.ncsc.nl/organisatie/nederlandse-cybersecurity-agenda.html) (translated from Dutch):

1. *Impact force in order: 'Government and businesses are able to offer an adequate response' 'with retention of basic values and privacy" (pp 19-20).*
2. *International peace and security in the digital domain: 'The Netherlands promotes international legal order in the digital domain, including the safeguarding of human rights' (page 23).*
3. *Digitally safe hardware and software: 'Users must be enabled (empowered) to understand the digital safety of hardware and software' (p. 27)*

Moreover, we used topics of the National Cyber Security Research Agenda III (https://www.dcypher.nl/national-cyber-security-research-agenda-iii-ncsra-iii-2018) as input as well:

1. *Design: 'Striking the right balance between usability and security is a recurring and crucial challenge in design' (p. 10)*
2. *Defence: 'Dramatically increase efficiency and effectiveness: 'speed at which attacks are detected, understood and responded to' (p. 14)*
3. *Attacks: 'Need to better understand 'hardware-software-people systems', especially the 'human factor' in cybercrime and cybersecurity' (pp. 19-20)*
4. *Governance: 'We tend to ignore that for this end-user failure to be so consequential, many other actors have already failed to adopt sufficient secure designs or defensive measures' (p. 24)*
5. *Privacy: 'Collecting large troves of data has economic value and improves the functionality … and national security policies, while privacy risks and damages are uncertain and distant' (p. 28)*

Findings from the workshop

During the workshop the following six ideas were generated, explored and discussed (A-F):

A. Quality Mark for Internet of Things Devices

People are increasingly putting IoT devices in their homes and businesses, from robot vacuum cleaners to fish tank thermometers and baby watching cameras. There are many vulnerabilities associated to these devices:

- People don't bother or forget to change the default password ("00000")
- They don't update the firmware, or the device does not support updating its firmware
- There is little incentive for producers to improve this—they often compete on price
- These devices can be accessed and used as stepping stones, to enter a company's intranet (e.g., the fish tank thermometer https://thehackernews.com/2018/04/iot-hacking-thermometer.html)
- Or these devices can be turned into a botnet, and can be thus be used for, e.g., a DDoS attack

A potential solution would be a quality mark for IoT devices, overseen by an independent government agency (e.g., Autoriteit Consument en Markt); this Quality Mark would then ensure measures like: this IoT device requires using a password, other than the default "00000"; or there will be firmware updates for five years into the future. There are quality marks for security of food, for health and safety of products, so why not for cybersecurity of IoT devices?

Values at stake:

- Freedom: Producers and vendors of IoT devices can perceive this measure as infringement of their freedom. There is, however, a history of successfully introducing measures for safety, e.g., safety belts in cars. If everybody needs to comply, they do not disturb the free market.
- Equality: Equality is likely to improve through this measure. There are currently risks of inequality regarding costs (less expensive devices are likely to be less secure) and regarding skills (people with less skills are less able to use these devices securely). When all IoT devices are made more secure, for this Quality Mark, these inequalities will diminish; less expensive devices will become safer and people with less skills will be able to use these devices safely.

Considerations:

- Legality and legitimate aim: This measure would comply with the rule of law, and it would have moral legitimacy; citizens can expect protection from being harmed through their IoT devices, and the government (at state level or European level) can be expected to take such a measure;
- Necessity, adequacy, proportionality: The risks of unsecure IoT devices are large and are likely to increase, and measure must be taken. A Quality Mark is likely to be an effective and efficient measure—it is relatively simple and small that can have a relatively large and positive impact.
- Authority, transparency, oversight: This measure can be best implemented on the state level—this is faster than working on the European level. Moreover, it will need to be designed and implemented through a transparent process and involve some independent government agency, in order to ensure public oversight.

B. Protection Services by the ISP

Another potential solution for the vulnerability of IoT devices (or any networked device) is that the ISP (the company that puts the router in people's homes and in businesses), monitors the addition of any new device to the home's or business' network. If the ISP recognizes the device as safe, it allows it to connect fully. If, however the ISP recognizes the device as unsafe, e.g., because it has outdated firmware, then it warns the user: "We detected a device with outdated firmware. We have put it in a walled garden; it can now only receive data, but not send any data. You need to update the firmware [instructions]; after that, it will be added to the network so that it can both receive and send data."

This measure is imagined as a value added service by an ISP. We can imagine, e.g., that ISPs in the higher end of the market will offer this service as an extra benefit. Other ISPs, e.g., at the lower end of the market, are less likely to offer this, or will offer it later on, after it has become a commodity.

Values at stake:

- Freedom: Such a measure concurs with a free market: with companies' freedom to develop and market specific services, and with people's freedom to choose and buy specific services.
- Equality: The value of equality, however, can be threatened by such a measure. It could exacerbate the digital divide. In the worst case, it could lead to a situation where people who can afford a high-end ISP have better protection against cyberattacks, whereas people cannot afford this are vulnerable to cyberattacks.

Considerations:

- Legality and legitimate aim: It would be legal for an ISP to offer such a service. There could be questions regarding moral legitimacy, e.g., when a company offers different services for different segments of the market, and then offers this extra protection only in its services for higher-end segments and not in its services for lower-end segments—people (or journalists) can easily 'discover' this and critique it ("You are effectively denying protection to less-paying clients").
- Necessity, adequacy, proportionality: This measure may look to many as not very necessary, as a 'nice to have' extra service. If implemented in a user-friendly way (which would largely depend on the people and processes of the ISP offering the service), then it is likely to be both effective and efficient.
- Authority, transparency, oversight: This measure can be best implemented on the level of the individual ISP. It would then fall in the domain of free market economy, with the risks of specific firms gaining (unfair) strategic (monopolistic) advantages; there would thus be a need for transparency or public oversight, with, e.g., fair communication and terms and conditions.

C. Cybersecurity Basic Insurance

It may be worthwhile for citizens or (small and medium) enterprises to buy a service for cybersecurity. In addition, it would be possible to buy a cybersecurity insurance to go with this service. This would fit in a free market, where both sellers and buyers are free to engage in transactions. It would be comparable to booking a trip or a holiday—and to book a travel insurance to go with this trip or holiday. However, there is a risk that the coverage or the conditions of such an insurance are out of line with what buyers thought that it would cover. There is sometimes a lot of fine print, which buyers are inclined to not read properly or thoroughly.

In order to reduce this risk, it could be a good idea if some independent agency (maybe even an agency of the national government) sets minimum requirements for such a cybersecurity insurance. This would protect buyers against having expectations that are too high or not in line with the fine print. This insurance would not be obligatory (freedom to choose is not compromised). The only thing this agency does is set a minimum standard; it prescribes a Cybersecurity Basic Insurance. Similar to the way that the Dutch national government prescribes the contents of a Basic Health Insurance (which is, by the way, obligatory; whereas the Cybersecurity Basic Insurance is voluntary).

Please note that such an insurance cannot be bought separately; it is an add-on on some service.

The insurance would promote preparedness in that it will require of citizens or enterprises to comply to specific guidelines, e.g., using strong passwords, updating software, making backups. It would make

sense if these measures are exactly in line with the service they subscribe to. If they then become victim of a cyberattack, it is reasonable to expect the insurer to repair the damage and pay-out.

Values at stake:

- Freedom: As long as this insurance is not at stake, freedom of both sellers and buyers is not at stake. Freedom would, however, be at stake if there is a whole lot of information that an insurer wants to see before getting the insurance—this would corrode freedom in terms of privacy.
- Equality: Having a standard for a Cybersecurity Basic Insurance could improve equality; it would enable also people with relatively less money to spend and less computer/security skills to protect themselves appropriately, at a fair price and with little skills involved.
- Solidarity: As with many forms of insurance, this type of insurance will work best if it is based on solidarity; if money is collected from a diverse group, in which setbacks are randomly distributed, and pays-out to those who are entitled. An insurance without solidarity will work less well; it will charge more of those with high risks and charge less for those with lower risks—which would undermine solidarity.

Considerations:

- Legality and legitimate aim: Such an insurance would comply to the rule of law.
- Necessity, adequacy, proportionality: Such an insurance would help people and enterprises to follow the guidelines for preparedness—they will be helped through the service they buy and they will need to comply if they want to be eligible for help and pay-out in case of an attack.
- Authority, transparency, oversight: The description of such an insurance can best be done on the national level, and needs to be transparent.

D. Make Apps Obligatory

People are increasingly using their smart phones for all sorts of transactions or payments. This makes it attractive to criminals to hack into these smartphones and transactions. In general, it is more safe to use a dedicated app, e.g., for banking, than to use a browser and a webpage. The app will typically have end-to-end encryption and the app can be managed and updated, e.g., by the bank. Using a browser and a webpage, on the other hand, can be less safe; e.g., the browser can be fooled to think it is connected to the bank when in fact it is not.

A solution would be to make the usage of apps obligatory; to make the service only accessible for apps, not as a webpage. This will result in a tension between security and customer-friendliness within the company issuing the service: the security people will support the app (because it is more secure), whereas the marketing people will promote the webpage (because it is more easily accessed for a first time or occasionally; a customer does not need to download, install and configure the app).

Similarly, one can obligate employees (of a bank or of any office) to use a standard laptop (supplied by the company) and to configure the intranet in such a way that it can only work with this laptop and via a VPN. No ‘bring your own device’; any other device will not be given access to the network.

Values at stake:

- Freedom: One can argue that making the usage of apps (instead of a webpage) or a standard laptop (instead of another device) corrodes freedom. On the other hand, one can argue that this freedom is only marginally corroded; downloading, installing and configuring an app takes a couple of minutes. Carrying a laptop for work is not a big deal. The app and the laptop are secure and easy-to-use alternatives, and do not really corrode freedom.
- Equality: Having all customers use the same app or having all employees use the same laptop is likely to contribute to equality. E.g., because any (implicit, unintended) inequalities based on the usage of different would be eliminated (which will need oversight—see below).

Considerations:

- Legality and legitimate aim: If the implementation does not violate prior commitments (and, e.g., give people ample time to switch) then it would fit with the rule of law.
- Necessity, adequacy, proportionality: From the perspective of the user, it is questionable whether this measure would be effective and efficient. If they use 40 services on their phone, of which 20 via a webpage and 20 via an app, they will still be vulnerable. On the other hand, the measure is likely to improve the company's cybersecurity because it would reduce the risks of users infecting their service by using a corrupt browser.
- Authority, transparency, oversight: There would be a need for public oversight, e.g., on the national level by an independent authority, to ensure, e.g., non-discrimination.

E. Better Communication for Learning

Citizens and (small and medium) businesses try to improve their preparedness (or resilience) for cybersecurity; they try to prevent (anticipate), they try to manage the attack (detect and react and repair) and they try to learn from it, to 'bounce back' stronger (in the vocabulary of resilience). However, they often do not have many clues as to what happened, what they could have done better and what they can do better a next time.

A potential solution would be improved communication to citizens and small businesses. E.g., an explanation like "there was an X malware, which entered your computer via Y email, which caused Z damage", and instructions for what to do better, like "if you see A, do B, and never do C". It's like a home burglary: the police comes and sees the lock on the front door; they will then advise you to buy a better lock, or use the lock better, e.g., turn the key one more round.

It would make sense if the national government provides general information, e.g., on how to repair and prevent cyberattacks (https://crisis.nl/wees-voorbereid/cyberaanval/), and if companies provide more detailed information, e.g., an ISP can provide information on an attack that happened via their servers or routers. It is, however, possible that firms label their own solutions as "secure" and their competitors' solutions as "insecure"—either out of genuine concerns for security and disagreement about what is "(in)secure", or out of a more or less malicious motivations to denigrate competitors. This will require some oversight (see below).

Values at stake:

- Freedom: Better communication will promote freedom because more knowledge leads to more freedom, provided that knowledge is available, accessible and usable for all people (see next bullet).
- Equality: This communication will need to be made available, accessible and usable for all people—it would corrode equality if the communication is only available, accessible and usable to specific, privileged groups.

Considerations:

- Legality and legitimate aim: General information can be expected to come from the national government. Specific information will need to come from commercial parties involved.
- Necessity, adequacy, proportionality: General information is likely to be only partly effective and partly efficient—it is not necessarily a lack of information; it's more a lack of motivation (see next bullet). It remains, also, to be seen whether companies, such as ISPs, would be able and willing to provide detailed and specific information to people (see above).
- Authority, transparency, oversight: This is a relatively lightweight measure, which does not need much legitimate authority or public oversight.

F. Motivate People to be Better Prepared (more than 'only inform')

Some people are not aware of cyber-risks and have no knowledge on what to do for preparedness; these people need information (see previous bullet). Other people are aware of the risks and have knowledge for preparedness; however, they do not follow-up practically on this knowledge. This is like living next to a river and being aware of the risk of flooding and knowing that you need an emergency kit—but not having prepared such an emergency kit, so that in case of a flood you are not prepared. In very general terms, what is missing is not information, but motivation to act.

A potential solution is to develop a program to motivate people to be better prepared, e.g., based on insights from (social or economic) psychology, like 'nudging'.

Values at stake:

- Freedom: A program to motivate people to change their behaviour will need to be very careful not to invade on people's freedom. On the other hand, all sorts of organizations and companies are attempting to influence people's behaviour (often opaquely but successfully nevertheless).

Considerations:

- Legality and legitimate aim: A program like this could be initiated either by the (national or local) government, or by a commercial party.
- Necessity, adequacy, proportionality: It is necessary to do more than provide information. Practically trying-out would be needed to see whether and how this actually helps people to change their behaviours.
- Authority, transparency, oversight: This measure would aim to make people change their behaviours (more than 'only inform'), which is less lightweight—some assessment of the

organization that offers the program (government or company) will be needed, e.g., to see whether it is seen as a legitimate authority to provide this program.

Conclusions

In the workshop, we explored several ways to improve the preparedness for cybersecurity. We generated six ideas for practical measures to promote preparedness in people and in (small) businesses. Different agents would be involved in such measures: government agencies, companies like ISPs, and citizens have different roles and responsibilities. Furthermore, for each of these ideas we explored key values, like freedom and equality, and criteria, like legality, necessity, adequacy, proportionality, and the need for transparency and oversight. These values and criteria will need to be taken into account carefully when designing and implementing such measures.

This workshop was to some extend also an experiment to see whether a discussion of such values and criteria can support the creative process of envisioning and designing such measures. The idea is to take into account 'ethics', ethical issues and societal implications, at the start of a creative process, as productive tools—rather than postponing 'ethics' until implementation (when the design-work is already done). Although this workshop was limited in its scope, we are positive about the productive potential of taking into account 'ethics' early on, in the creative and explorative phase.