Safety and Reliability – Safe Societies in a Changing World – Haugen et al. (Eds)
© 2018 Taylor & Francis Group, London, ISBN 978-0-8153-8682-7

Building cyber resilience through a discursive approach to "big cyber" threat landscapes

T.O. Grøtan
SINTEF Technology and Society, Trondheim, Norway

ABSTRACT: Cyber safety, security and resilience of Critical Infrastructures (CI) and critical societal functions is a contemporary challenge. To understand the bigger picture, we may build composite threat landscapes in which vulnerabilities and threats combine and travel across distinct domains between which expertise, competence, experience and knowledge horizon related to safety, security and risk may differ substantially. Additional sensitization towards emerging cyber threats is however needed. Inspired by the post-normal "science of what-if", the "BigCyber" model advance threat landscapes further into sensitivity to hidden, dynamic and emergent vulnerabilities. The approach is exemplified in terms of smart metering of household electricity consumption. The need for discursive support for different stakeholders relating to threat landscapes is identified, and a discursive framework for stepwise nurturing of polycentric governance is outlined. The framework can also be used to elaborate and support the idea of resilience landscapes of autonomous entities, facilitating a polycentric approach to cyber resilience.

1 INTRODUCTION

The potential consequences of failure and disturbance of Critical Infrastructures (CI) and societal functions (e.g., energy, water, transport, and logistics) depending on Information and Communication Technology (ICT) are frightening and potentially devastating. The overall risk picture is increasingly blurred, mixed and constantly evolving. It is difficult to maintain a sharp divide between the stable inside of a critical infrastructure, and a more innovative outside. Presumed motivations of potential adversaries and perpetrators span a wide range, encompassing cyber conflict and hybrid warfare, fake information, political influence, cyber-physical damage, cybercrime, sheer vandalism or teenager tricks. This adds to the existing prospects of the accidents, failures and unfortunate incidents in (already) complex systems. Perrow's (1984) notion of the "normal accident" is persistently hard to escape.

The Internet of Things (IoT) is already on the scene, offering new access (= attack) points, new magnitudes of automation and cyber-physical impact, but also boosting the ability to "informate" (Zuboff 1984); to generate electronic texts about the use of the infrastructure. Moreover, the "Internet of Everything" (IoE) has been coined as the "Big Other" surveillance capitalism (Zuboff, 2015), fueling a logic of accumulation. This is signified by the increasing rate of ICT systems rigged for collecting as much (surplus) data as possible. Vendors collecting extensive information from installations without the customer's consent, could be coined as the "industrial Big Other"

In the 1990's, the prospect of "trusted" computer systems prevailed. Today, few if any ICT systems are delivered with assurances that support this. Practically no ICT system, including CI, may preclude the possibility of intrusion, disturbance and hacking. Big-scale consumer innovations, e.g. autonomous cars and home appliances, are seemingly always lagging in computer security. Some voices even claim that "computer security is broken from top to bottom" (Economist, 2017).

Potential countermeasures are often invasive, e.g. on privacy, often unduly playing on strings of fear and anxiety. Public initiatives, e.g. from the EU (Galbusera and Giannopoulos, 2016) aiming for public, semantic web descriptions of critical infrastructures may also be exploited to enable sophisticated attacks.

We cannot expect of holistic, cross-nation, cross-sector approaches to these challenges. The obstacle is not just the tremendous information coordination challenge, but also the incommensurate and diverse motives and objectives across boundaries of private vs public, classified vs unclassified, national vs international. Information cannot be shared, nor trusted, in one "heap". Motives and objectives are incommensurate, increasingly located in an atmosphere of post-fact attitudes, fake news, and information warfare targeting societal trust, in which even security agencies may find it difficult to navigate.

This fundamental challenge demands an attempt of imagining the inconceivable. Societies, organizations and stakeholders habitually directs their hope and faith for dealing with such challenges to risk management and governance, but these are increasingly acknowledging their limitations. Illustratively, a new Specialty Group (SG) on resilience analysis was approved by the Society of Risk Analysis (SRA) Council on December 10, 2017.

In the following, a diverse portfolio of strategies and approaches that can be utilized at several levels, from the national regulator to the infrastructure owner and stakeholder is proposed. The key issues are about building *threat landscapes* to increase sensitivity to hidden, dynamic and emergent ("*h*/*d*/*e*") vulnerabilities and couplings, and to employ the concept of resilience in a polycentric manner catering for diversity, rather as a system-wide property on uniform terms.

An example is offered: smart household electricity metering as part of smart grids. Energy companies strive to use technology to innovate their customer relations, technical maintenance and grid stability, fearing cyber threats, but also fearing a sudden, technology-driven meltdown of their business models.

2 THREAT LANDSCAPES—AND BEYOND

2.1 *Threat landscapes*

Risk management is traditionally not possible without making demarcations about a system regarding boundaries, threats, vulnerabilities, key events, and other inventories (e.g., acting subjects). In today's complex cyber-inflicted systems, such presumptions become increasingly difficult. *H*/*d*/*e* couplings between parts that we traditionally would prefer to keep apart for analytical clarity, or events and conditions that would be considered as unlikely or even irrelevant in conjunction, challenge organizations' and societies' experiences, capabilities and skills regarding imagination as well as actual resilience towards disturbance and surprise.

A societal perspective will have to address the b*igger picture* by recognizing and combining multiple, distinct domains of expertise, competence, experience and knowledge horizons related to, e.g., safety, security, resilience, threat and risk. In this paper, any such distinct domain is "squared out" as a picture, with a frame representing demarcation of inside vs outside, however with the premise that there *may* always be some relevant knowledge missing.

A key challenge is that due to the diversity and h/d/e ICT-induced couplings of physical as well as logical nature, "pictures" may suddenly turn out to be be flawed, and the new threats may travel across such experience-based boundaries in unprecedented ways. The understanding of such composite threat landscapes require methods beyond the practices used to address single domains. Although it is likely that the (more or less professional) risk management approaches per se do not vary dramatically across such "squared" frames, it is likely that the pragmatic knowledge horizon of each domain, e.g., the sensitivity to different phenomena and the ways information and knowledge is recognized, collected, combined and appreciated, will differ substantially more.

Due to the presumed heterogeneity of the total landscape, it is held unlikely that a joint holistic picture of threats and vulnerabilities can be comprehended from a single knowledge horizon. Hence, it is presumed that the "visible landscape" that can be created and shared between domains is constituted by several "squares", each of which representing a specific horizon of knowledge-gathering ("knowledging") strategies and actual experience. To be able to construct such a landscape, three issues are crucial:

1. Explication of the boundary conditions for each horizon "squared out" (Figure 1) in terms of the frame description, the demarcations of the validity of the inside, and the indicators of its saturation (that is, when it cannot accommodate more issues, without losing its pragmatic meaning)
2. the characteristics of overlap zones and the corresponding h/d/e vulnerabilities and couplings that may enable threats to propagate
3. The joint acknowledgement that single frames, as well as their intersections, are not only uncertain, but also influenced by a background landscape encompassing h/d/e phenomena.

The labyrinth background in Figure 1 signifies the persistent hermeneutical challenge of a "moving horizon" (Gadamer 1992) facing each "squared" horizon, as it encounters new phenomena and contesting horizons through the overlap zones.

The resulting threat landscape metaphoric hence implies a loss of traditional presumptions of clear-cut responsibility and authority traditionally associated with single pictures/frames, but also an increased sensitivity to other horizons of understanding.

For taking advantage of this landscape metaphoric, each knowledging agent or community must acknowledge the need to understand the foundations of its own horizon, and be able as well as willing to take a closer look beyond its prevalent presumptions.

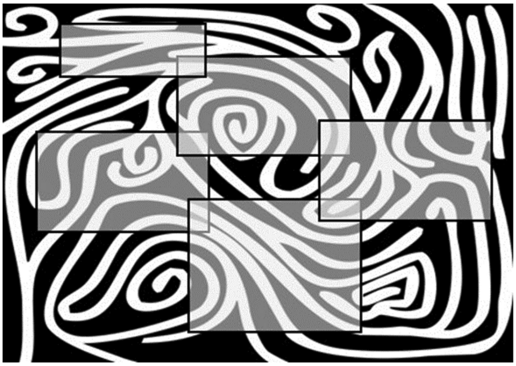

Figure 1. Overlapping threat pictures constituting a threat landscape on a labyrinth background (Grøtan and Antonsen, 2016).

In this way, the threat landscape metaphor may be used to build a "bigger picture" including h/d/e couplings between distinct domains, among which expertise, competence, experience and knowledge horizon related to safety, security, threat and risk are not necessarily commensurate. To establish the grounds for extended understanding of the surrounding landscape, each agent may take advantage of the "take it to the limits" approach (Grøtan and Antonsen 2016) in which a sequence of issues is raised to encircle the boundaries and the saturation points of each frame, and open up for inputs from other domains.

2.2 *"What-if": Sensitization and weak signals*

The threat landscape approach above is primarily useful for utilizing past experience and existing knowledge from professional domains, looking for new combinations, and for revealing or spotting h/d/e vulnerabilities before they have negative impact.

However, many recent events illustrate that cyber (h/d/e) vulnerabilities emerge as a big surprise or a "black swan". A recent example is social media allegedly being used for political communication, tipping elections (Guardian, 2017), indeed exceeding what may be anticipated by means of traditional scientific approaches. The public sphere is very likely to be affected by the consequences, and involved in the key phenomena, e.g., as actually being the product, not the customer, for "Big Others". The threat landscape approach per se may thus not be enough. The residual challenge is thus to be able to raise and pursue the question "what-if" based on hints, weak signals or sheer imagination, and make a serious judgment in time on issues that normally might be discarded as belonging to a risk distribution tail. Also, the "layman" horizon should be included in the process.

To address this residue, inspiration is here gathered from the "post-normal science" (PNS) (also denoted the "science of what-if") introduced by Funtowicz and Ravetz (1993) and Marchi & Ravetz (1999), setting out to resolve a science in crisis (sic!).

Kønig et al. (2017) identify the conditions characterizing a post-normal situation: Irreducible complexity, deep uncertainties, multiple legitimate perspectives, value dissent, high stakes, and urgency of decision-making. The PNS goal is not to attain certain knowledge, but quality, a more robust 'science for policy'. Pointing to how politicization of science renders classical Mertonian scientific norms invalid, they identify an ethos for PNS which they denominate TRUST (Transparency, Robustness, Uncertainty management, Sustainability, and Transdisciplinarity), considering this a nexus for reflexivity practices. They propose that the public trust in science advice can be restored through the PNS ethos.

PNS is also portrayed as "both *descriptive* (describing urgent decision problems – post-normal issues – characterized by incomplete, uncertain or contested knowledge and high decision stakes and how these characteristics change the relationship between science and governance) and *normative* (proposing a style of scientific inquiry and practice that is reflexive, inclusive and transparent in regards to scientific uncertainty and moving into a direction of democratization of expertise)" (Strand 2017).

Here, the PNS challenge is responded to in a more meagre and restricted way; 1) by urging for sensitivity to weak signals, and 2) the proposition of a cyber-vulnerability sensitization model that hopefully make sense to professionals and laymen alike. Hopefully, this is a contribution to the PNS urge to invite "extended peers" into the conversation. Ubiquitous cyber vulnerabilities, and the hope of cyber resilience, should not only be based on a discourse among professionals; ultimately it involves us all.

The turn towards PNS for inspiration, and the return to the less ambitious sensitization model presented below, is thus a natural next step from the idea of the threat landscape as a vehicle for joint comprehension and discourse based on validated of, or even sense-*making* from, weak signals. The notion of "weak signal" is thus not confined to uncertainty within a familiar domain, but include the possibility that something radically outside the normal frames of reference may "travel" trough the landscape, with significant impact at unexpected places.

2.3 *The BigCyber sensitization model*

This sensitization model is intended as a generic tool to support a balanced approach to understanding the temptations as well as the possible drawbacks related to utilization of the ever-evolving "cyber space".

2.3.1 *Underlying and formative issues*

2.3.1.1 Potential conflict in cyber space

The actors who own and operate critical infrastructures are usually not directly involved in (military) cyber conflict scenarios, they have traditionally not been seen as military actors. Still, they may be targets for offensive cyber weapons in a potential conflict situation. By making attacks on critical infrastructure from afar technically possible, digital technology also make these types of attacks feasible. It is therefore important that these actors think about the possibility of being targets, and prepare accordingly. An attack of this type could be intended to simply disrupt services, sabotage or even cause physical damage. E.g., Since being coined by CIA Director Leon Panetta in 2016, there has been a persistent concern in the US regarding a potential "Cyber Pearl Harbour" attack.

2.3.1.2 The Internet of Things (IoT)

IoT implies a network of objects able to collect data through embedded sensors and exchanging this information via the internet, but are notoriously hard to secure, and even hard to update when needed.

Both intended, malicious cyber threats and unintended system failures and vulnerabilities of IoT dispersed throughout a CI may lead to severe disruptions in cyber physical systems. In 2016, we also experienced a hint of the future, as the recognized scale of DDoS attacks increased dramatically due to the broad availability of tools for compromising and leveraging the collective, offensive firepower of IoT devices—poorly secured Internet-based security cameras, digital video recorders and Internet routers (Guardian, 2016). The intentions and motives behind may be related to crime and hackers, ranging from teenagers' ploys via organized crime to state actors, but also to cyber conflict and hybrid warfare.

IoT thus sparks the ability to "informate", to generate electronic texts around the use of the infrastructure and technology, boosting the "Big-Other" logic of accumulation.

2.3.1.3 From IoT to Internet of Everything (IoE)

As more and more personal information is being made more or less public, and the possibility for combination increases, a new form of information economy emerges. Zuboff (2015) describes the emergent logic of accumulation in the networked sphere as an "Internet of Everything" (IoE) in which personal information becomes a commodity of high value for a wide range of (unknown) users. This radical new form of surveillance capitalism aims to predict and modify human behavior as a means to produce revenue and market control. Zuboff (2015) launches the need for an 'information civilization' addressing the challenges from "Big Other": "a ubiquitous networked institutional regime that records, modifies, and commodifies everyday experience from toasters to bodies, communication to thought, all with a view to establishing new pathways to monetization and profit" (Zuboff, 2015).

Such an "information civilization" requires a new comprehension of cyber safety and security, including the multifaceted concept of resilience.

2.3.1.4 The lack of assurances

Given the high ambitions related to evaluation criteria for "trusted" computer systems a couple of decades back, there is a striking contemporary silence and numbness related to the lack of assurances about vulnerability of critical computer systems, at least in the non-classified domain. The infamous Stuxnet incident has demonstrated that a widely used industrial control system platform can be used to launch very intricate attacks that are very hard to spot. This is not only about "zero days", it is also about an inherent technological brittleness, and the possibility that industrial plants such as windfarms (Staggs et al. 2017) or smart metering systems (Hansen et al. 2017) demonstrably can be "hacked", with potentially severe consequences. This is also about a flawed marketplace that does not care to ask for such assurances at all, or just to a very minor degree.

2.3.1.5 Privacy

The Norwegian Data Inspectorate have just recently aired their concern regarding the implications of this, and The Norwegian Consumer Council is worried about privacy and consumer rights in a situation where such consumer data has become a "goldmine" for infrastructure operators. The Norwegian telecom operator Telenor is making data from the cellular network to a commodity under the label "mobility analytics". In the US, a new bill is criticized for being a lift of existing legislation that "not only gives cable companies and wireless providers free rein to do what they like with your browsing history, shopping habits, your location and other information gleaned from your online activity, but it would also prevent the Federal Communications Commission from ever again establishing similar consumer privacy protections". It can be doubted whether the individual customer will be able to value his/her privacy sufficiently in relation to the "benefits", or the sheer volume of "user agreements" that are offered.

2.3.1.6 Enter psychology

1. Big Five in Big Data

Psychoinformatics (Montag et al., 2016) is a discipline on the rise. The "Big Five" model has been a prevalent model for psychological profiling, with alleged predictive power on human behaviour and influence. Recently, the Big Five model has been a driving force in "Big Data" attempts of collecting enough data to reveal patterns from which predictions about human behaviour become quite precise). Some findings seem to suggest strong correlations between Big Five parameters and social media (e.g., facebook) data. E.g., an average of 68 "facebook clicks" seemed to be enough (in 2012) to predict colour of skin, sexual preference, political preference, intelligence, religious belief, use of alcohol/tobacco/drugs, or of having divorced parents, with reasonably high confidence (Grassegger & Krogerus, 2018). With more data, the model predictions beat the assessments of a person from colleagues, friends, parents and spouse. Ultimately, the smart phone is an "enormous psychological questionnaire" feeding us (or someone) with more and more detail. With more information, the prospect is raised that somebody could know "more than the informant think they know about themselves". Inherent in this is the assumed ability to predict an informant's response to a condition/situation.

But it also works the other way around: the user data can also be used as a filter to find and track down users/individuals with specific personality details; providing a method to "profile" people without themselves knowing. It is claimed that this has been used recently in political marketing/communication, by "micro-targeting" through assessments of personalities through Big Five and digital footprints. From which, political messages are organized and based on psychometry rather than demography, by, e.g., designated "messages" as personality-adapted advertisements or "news" (not necessarily "fake"). "Dark posts" are paid fb ads exclusively in the news feeds to users with specific personalities. It can also be about microscopic variations in the same message to accomplish psychological effectiveness, headings, colours, captions, stills or videos, targeting villages, neighbourhoods, or individuals differently. Hence, digital footprints become "real humans" with worries, needs, interests and addresses.

2. Cyber psychology in change

Another issue with possibly unprecedented implications is the potential implications of how digital omnipresence leaks into and potentially changes our psychology as users and operators, e.g. in terms of increased conformity (Størseth 2013).

2.3.2 *The BigCyber sensitization model*

The Big Cyber model summarizes the key issues at large, as illustrated in Figure 2. The model comprises five different "Janus-faces", each of which offering a huge benefit (inside of the dotted pentagon), as well as conducing a severe downside (outside of the dotted pentagon) that can be viewed as an h/d/e threat or vulnerability.

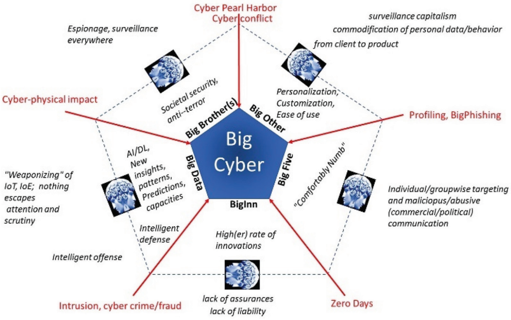
Cyber Pearl Harbor
Cyber conflict
Espionage, surveillance everywhere
surveillance capitalism
commodification of personal data/behavior
from client to product
Cyber-physical impact
Societal security, anti--terror
Personalization, Customization, Ease of use
Profiling, BigPhishing
Big Brother(s)
Big Other
Big Cyber
Big Data
Big Five
BigInn
AI/DL, New insights, patterns, Predictions, capacities
"Comfortably Numb"
"Weaponizing" of IoT, IoE; nothing escapes attention and scrutiny
Individual/groupwise targeting and maliciopus/abusive (commercial/political) communication
Intelligent defense
High(er) rate of innovations
Intelligent offense
Intrusion, cyber crime/fraud
lack of assurances
lack of liability
Zero Days

Figure 2. The BigCyber sensitization model.

BigBrother(s) may offer comfort and security in times of crisis and terror, but are giving themselves rather free passes to track down and inflict harm on any instance or person that may be regarded as a present or potentual adversary. There are no international agreements on ethical conduct of cyber offense.

Personalization and customization of services offers ease of use. But the backside is that we are enrolled into the **BigOther** surveillance capitalism (Zuboff 2015) without being properly asked or informed; "users" are transformed to products and monetized behavioral commodities in a digital economy.

BigData coupled with artificial intelligence and machine learning promise an endless range of new insight and capabilities, but these are not reserved for the "good" purpose. What if the key ideas of "insurance" are jeopardized? Intelligent offense towards CI and ICT systems is as likely as intelligent defense.

The **BigFive** personality model can probably make us even more comfortably numb while effortlessly harvesting the benefits of cyberspace. Will we be able at all to resist the narrowed "alternatives" presented? Will we develop a "cyber psychology" that enables us to recognize and deal with commercially and politically motivated communication?

This is also about an aggregated, unevenly distributed **digital economy and power**. BigOther will have supreme power to utilize BigData as well as BigFive. Evry cyber innovation is aiming for sale, and BigOther is loaded with cash and ready to buy any advantage and "edge" available.

Societies, organizations as well as individuals are always hungry for the **BigInn**(ovation). The lack of basic assurances are hardly noticed, except for the invitation to become an "update junkie", and that the computer industry is not subject to anything near the liability issues that, say, automakers or pharmaceutical industries must consider. Also, outsourcing with fragmented managerial accountabilities is a too easy escape when ambitions of digitalization exceed available competence to deal with the vulnerabilities.

The BigCyber model support understanding of exposure to unfamiliar intentions and motives, and of new attack surfaces and vectors, e.g., cyber-physical impact, small and large, massive profiling, crime and intrusion and an endless stream of "zero days".

3 EXAMPLE: SMART METERING

A smart meter is a physically separate device designed with encrypted communication between the energy supplier and the customer for regular metering at, e.g., an hourly basis. In one way, the Smart Meter is just another Industrial Control System (ICS) or Supervisory Control and Data Acquisition (SCADA) system that is a precondition for even preconceiving the idea of a smart grid, depending on control functions and measurements at an unprecedented scale.

As illustrated in Figure 3, the smart meter also has a "private" physical connector (in Norway denoted a "Home Area Network" (HAN) port) that enable third parties, e.g., providing "smart home" solutions, to read metering data as part of their (innovative) services, connected to the internet. However, do we understand the potential threat landscape of this?

Smart metering is an entry point to the huge challenges of protecting the energy grid as a critical infrastructure. Concerns can be raised, independent on whether the connection is physical or not, on both unauthorised access and to whether the end user oversee the implications of granting additional connections.

The attractiveness of the electricity system for cyber attacks was demonstrated in Ukraine (2015 and 2016). Disruptions may range from massive shutdown (leading to imbalance and potential physical damage) or just poor quality (voltage/frequency). The potential for targeting vast numbers of smart meters simultaneously is demonstrated (Hansen et al. 2017). We have yet to experience the full damage potential, but in the UK, MPs were warned of sabotage threat from smart meter hackers. As experts said rogue programmers could target £11bn system, a massive shutdown will put enormous strain on both the supplier and consumer side (Financial Times, 2016).

3.1 *The microcosmic threat landscape of ICS*

We start by illustrating the potential of the threat landscape approach at a very small scale. Resting on a similar vocabulary employed by The European Union Agency for Network and Information Security (ENISA), the smart meter seen as an ICS/SCADA system, can be depicted as a "microcosmic" threat landscape in its own respect (Figure 4).

the approach is illustrated in terms of a workshop assessment of an industrial SCADA system in a networked context. The actual "squared" threat pictures (left side of Figure 4) are selected and derived from a similar approach by ENISA. The actual threat landscape composition was conducted as part of the (1st Annual) Workshop on Cyber Safety, Security and Resilience of Critical Energy Infrastructures, Oslo, Norway June 2016. Here, each threat picture was elaborated before combined into the landscape. Both the contents of each "frame" or "horizon", and their overlaps, turned out to be surprisingly complex, and did add weight to the suspicion that the ideal design does not cover every vulnerability in this (microcosmic) threat landscape".

3.2 *The BigCyber-sensitized threat landscape*

Can we conceive a bigger picture, a BigCyber-sensitized smart meter threat landscape?

In addition to necessary functionality for building of smart grids, the smart metering solution is also an excellent example of a connection to "Big

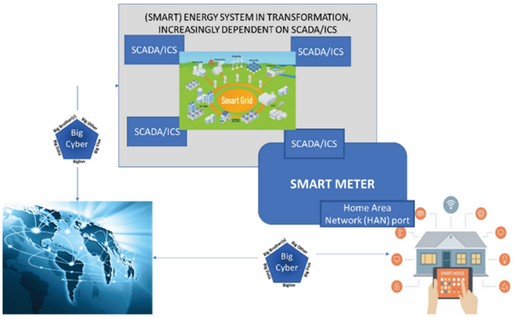

Figure 3. The Smart Meter as part of the Smart Grid.

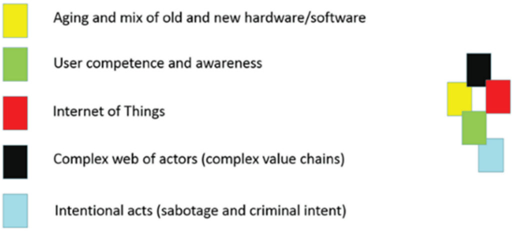
Aging and mix of old and new hardware/software
User competence and awareness
Internet of Things
Complex web of actors (complex value chains)
Intentional acts (sabotage and criminal intent)

Figure 4. "Microcosmic" ICS/SCADA Threat Landscape.

Other". The joint access to the HAN port it is also a source for building information about "energy behavior" with a huge commercial potential, especially when it is linked to other sources of individual and commercial behavior that can be used to profile targeted individuals or groups. The privacy issues are imminent, but a hostile "BigBrother" may in the ultimate case also weaponize this to trigger collective irregular consumer behavior, and target key personnel, with the intention of disturbing the energy system per se. Another possibility may be conceived through the infamous Stuxnet attack; either by (1) disturbing the crucial grid measurements in order to destabilize trust in grid operation, or (2) initiate (cyber-)physical damage by imposing electrical imbalances.

Hence, we may see the contours of new attack surfaces and vectors of both tangible and intangible kinds, that can be combined and cleverly orchestrated. Vulnerable equipment can be attacked, users and populations can be manipulated and influenced, and key personnel in protection of critical infrastructure services could also be specifically targeted as part of an orchestrated attack, e.g. with a criminal intent. For the defenders, a main vulnerability is the lack of acknowledgement of the coupling.

In Figure 5, a BigCyber-inspired Threat Landscape for smart metering is indicated. The prospects of "clinical" attack vectors, triggering of user behavior as part of attack, optimization of damage and targeting of key personnel on the inside, are simply not refutable one by one. Maybe not even in combination.

3.3 *Weak signals in sight?*

The "metering paranoia" threat landscape (Figure 5) is hypothetical. Are there weak signals that

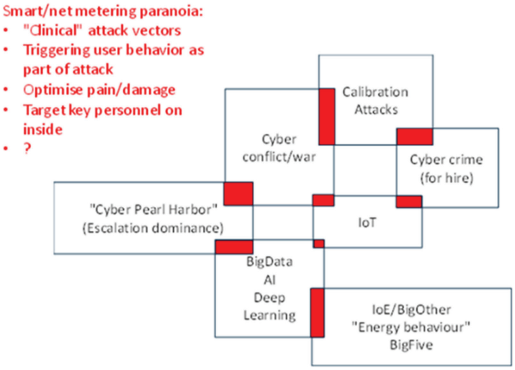
Smart/net metering paranoia:
• "Clinical" attack vectors
• Triggering user behavior as part of attack
• Optimise pain/damage
• Target key personnel on inside
• ?
Calibration Attacks
Cyber conflict/war
Cyber crime (for hire)
"Cyber Pearl Harbor" (Escalation dominance)
IoT
BigData AI Deep Learning
IoE/BigOther "Energy behaviour" BigFive

Figure 5. "Smart metering paranoia".

support the likelihood that it may manifest into reality?

- Banks in Asia are already using customers' smartphone data points, like how (often) they drain their battery, to determine whether they're eligible for a loan (CNN, 2016). Can electricity metering derived from smart houses contain behavioral data that could be matched with a personality assessment?
- Will customers care to use the new European privacy legislation to demand insight into smart metering data? Would the trivia of energy consumption draw the necessary attention?
- Energy companies are now increasingly concerned about disruptive competition. Who will take lead in offering homes and companies the dual role of producer and consumer, utilizing solar, wind, (virtual) batteries, e.g. in electrical cars, optimize the energy consumption in a market in which, e.g., consumption based pricing is replaced by capacity-based pricing? Will access to personal energy consumption be part of the "price"? Who will have the data edge in a new market environment? Will we see similar dynamics as when the "Flash Boys" (Lewis 2015) changed the stock markets by means of getting split-second advantages over other actors?
- The grid, however "smart", will still need some supervised electrical stability. Who will be responsible for managing this, with potentially severe consequences in terms of physical damage of electro-mechanical equipment. If for example Google offer an "integrated" energy system to "prosumers", would they care about the grid? If the risk towards the grid level of service is relocated, who will be in charge?

4 DISCURSIVE SUPPORT FOR POLYCENTRIC GOVERNANCE (PCG)

The challenges described above goes beyond the limits of safety and security as traditional disciplines. Petersen (2012) argue that we need an analytical approach "sensitive to conceptual change and diversity" that "enable us to identify innovations in political language" and "provide us with the ability to grasp new developments in the corporate, governmental or organizational conception of risk". There is thus a need for a step change in the way societies and organizations deal with cyber risk, from fragmented to polycentric risk governance (PCB).

The threat landscape metaphoric and the BigCyber sensitization model provide discursive support for PCG. E.g., as in the smart metering example, a regulator can be aware of privacy challenges, but must reach a risk-informed assessment,

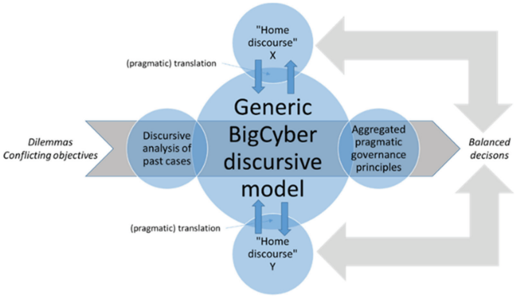
"Home discourse" X
(pragmatic) translation
Generic BigCyber discursive model
Dilemmas Conflicting objectives
Discursive analysis of past cases
Aggregated pragmatic governance principles
Balanced decisons
(pragmatic) translation
"Home discourse" Y

Figure 6. Discursive framework for polycentric governance.

based on current knowledge, without jeopardizing the objective of transforming the grid. We may expect that the regulator take part in a broader, responsible discourse, but we cannot expect them to be voluntarily taken hostage for issues beyond their primary mandate. Hence, we need a discursive framework that sensitizes not only academics and analysts, but also the actual decision makers/processes to the very same issues.

Petersen (2012) claim that "a conceptual discourse does not exist by itself; rather, it will always be defined in interaction with other discourses". Hence, a discursive framework will have to be designed with the following in mind: the users of the framework will come from unique and different "home discourses", and we should enable a sustained resonance between the "home" and the joint discourse, as participants move along their unique trajectories.

As indicated in Figure 6, several stakeholders, each of which bound to a home discourse, e.g., of privacy and consumer rights or of facilitation of smart grid development, can join forces, overlap horizons, share threat landscapes (TL) and challenge themselves and others by using the Generic BigCyber discursive model, which is the simplistic (and recursive) formula of

TL → BigCyber → TL',

as exemplified in chapter 3.

Using this discursive framework will contribute to an improved coherence between decisions made by different stakeholders. The "lay" perspective may be voiced through civic participation, NGOs, or proxied through agencies of consumer rights and privacy.

5 FROM PCG TO POLYCENTRIC RESILIENCE

During the past decade, the safety field as well as the societal security and disaster fields, have devoted attention to the concept of "resilience. However, the notion of cyber resilience demands more than a technological fix. Human and organizational issues are more inert than the technological, and also for cyber resilience we must respect the double-hermeneutic scientific principle of understanding *understanding subjects*, rather than explaining them as objects.

It is important that the concept is properly contextualized. Though it sounds normatively good, it carries no guarantee for success. It is an attractive idea that invites fallible practices, and hence it must be brought under managerial supervision, accountability and mandate. If not, we may invite expectations that will victimize those that are not able to thrive from being exposed to risk, or that do not possess the resources or skills in the first place.

We must take the notion of resilience seriously without depriving it from its content and origins through mere re-labelling of traditional risk management practices. Resilience is ultimately a matter of emergent, "bottom-up" and situated solutions to unique and idiosyncratic demands and situations rather that instrumental responses to stereotypical replications of former situations.

By implication of the above, cyber resilience must be translated to a scheme of composite protection comprising a diverse set of (resilient) entities that can be orchestrated to a certain degree. Grøtan and Bergström (2016) propose a theoretical foundation for exploring the concept of resilience landscapes; autonomous but interconnected resilient entities that forms a composite scheme of resilience. Such entities can utilize the same discursive structure as for PCG (Figure 6), and the evolving threat landscape can be a basis for dynamic interfaces and interactive patterns.

6 CONCLUSION

The threat landscape metaphoric and the BigCyber sensitization model is a promising approach that make sense in the smart metering case, and carries a potential for further application for the emerging cyber threat landscapes. The notions of polycentric governance and polycentric resilience landscapes are logical companions to the former, and both can benefit from the discursive support structure presented.

ACKNOWLEDGEMENTS

This paper is funded by the SAMRISK-II project New Strains of Society, under Contract no 238093/H20 with the Norwegian Research Council.

REFERENCES

Financial Times, web pages. 2016. MPs warned of sabotage threat from smart meter hackers. September 24, 2016.

Funtowicz, S.O. & Ravetz, J.R. 1993. *Science for the post-Normal age. Futures*, 25 (7) (1993), pp. 739–755.

Gadamer, H-G. 1992. Truth and Method. 2nd ed. Trans. Joel Weinsheimer and Donald G. Marshall. N.Y.: Crossroad.

Galbusera, L. & Giannopoulos, G. 2017. Exploiting web ontologies for automatic critical infrastructure data retrieval. Eleventh Annual IFIP Working Group 11.10 International Conference on Critical Infrastructure Protection. Arlington, USA, March 2017.

Grassegger, H. & Krogerus, M. 2018. The Data That Turned the World Upside Down. https://motherboard.vice.com/en_us/article/mg9vvn/how-our-likes-helped-trump-win, downloaded 2018–02–15

Grøtan, T.O. & Antonsen, S. 2016. Take it to the limits! Exploring the hidden, dynamic and emergent vulnerabilities of society. ESREL 2016: Taylor & Francis Group, London.

Grøtan, T.O. & Bergström, J. 2016. Calibrated resilience landscapes of composite protection: Theoretical grounding of an empirical approach. ESREL 2016: Taylor & Francis Group, London.

Guardian, The. 2016. DDoS attack that disrupted internet was largest of its kind in history, experts say. October 26th.

Guardian, The. 2017. Did Cambridge Analytica influence the Brexit vote and the US election? March 4th.

Hansen, Aa., Staggs, J. & Shenoi, S. 2017. Security Analysis of an Advanced Metering Infrastructure. . Eleventh Annual IFIP Working Group 11.10 International Conference on Critical Infrastructure Protection. Arlington, USA, March 2017.

Kønig, N., Børsen, T. and C.v Emmeche. 2017. The ethos of Post-normal science. Futures. Volume 91, August 2017, Pages 1–4.

Lewis, M. 2015. Flash Boys. A Wall Street Revolt. Norton Marchi, B., Ravtez, J: 1999. Risk management and governance: A post-normal science approach. *Futures* 31(7):743–757.

Montag, C. et al. 2016. Toward Psychoinformatics: Computer Science Meets Psychology. Computational and Mathematical Methods in Medicine. Volume 2016 (2016), http://dx.doi.org/10.1155/2016/2983685

Perrow, C. 1984. Normal Accidents: living with high-risk technologies. New York: Basic Books.

Petersen, K.L. 2012. Risk analysis–A field within security studies? Eur. J. Int. Relations, vol. 18, no. 4, pp. 693–717.

Staggs, J., Ferlemann, D. & Shenoi, S. 2017. Wind Farm Security: Attack Surface, Targets, Scenarios and Mitigation. Eleventh Annual IFIP Working Group 11.10 International Conference on Critical Infrastructure Protection. Arlington, USA, March 13–15 2017.

Strand, R. 2017. Post-normal science. In C.L. Spash (Ed.), Routledge handbook of ecological economics: Nature and society, Routledge, London, pp. 288–298.

Størseth, F. 2013. Digital culture conformity: contours of a 'new psychology' and its impact on safety. PSAM 2013, Tokyo, Japan, 14–18 April 2013.

Zuboff, S. 1984. In The Age Of The Smart Machine: The Future Of Work And Power.

Zuboff, S. 2015. Big other: surveillance capitalism and the prospects of an information civilization. *Journal of Information Technology*, 30, 75–89.

CNN. 2016. http://money.cnn.com/2016/08/24/technology/lenddo-smartphone-battery-loan/index.html

The Economist, April 2017. Computer Security is Broken from Top to Bottom.