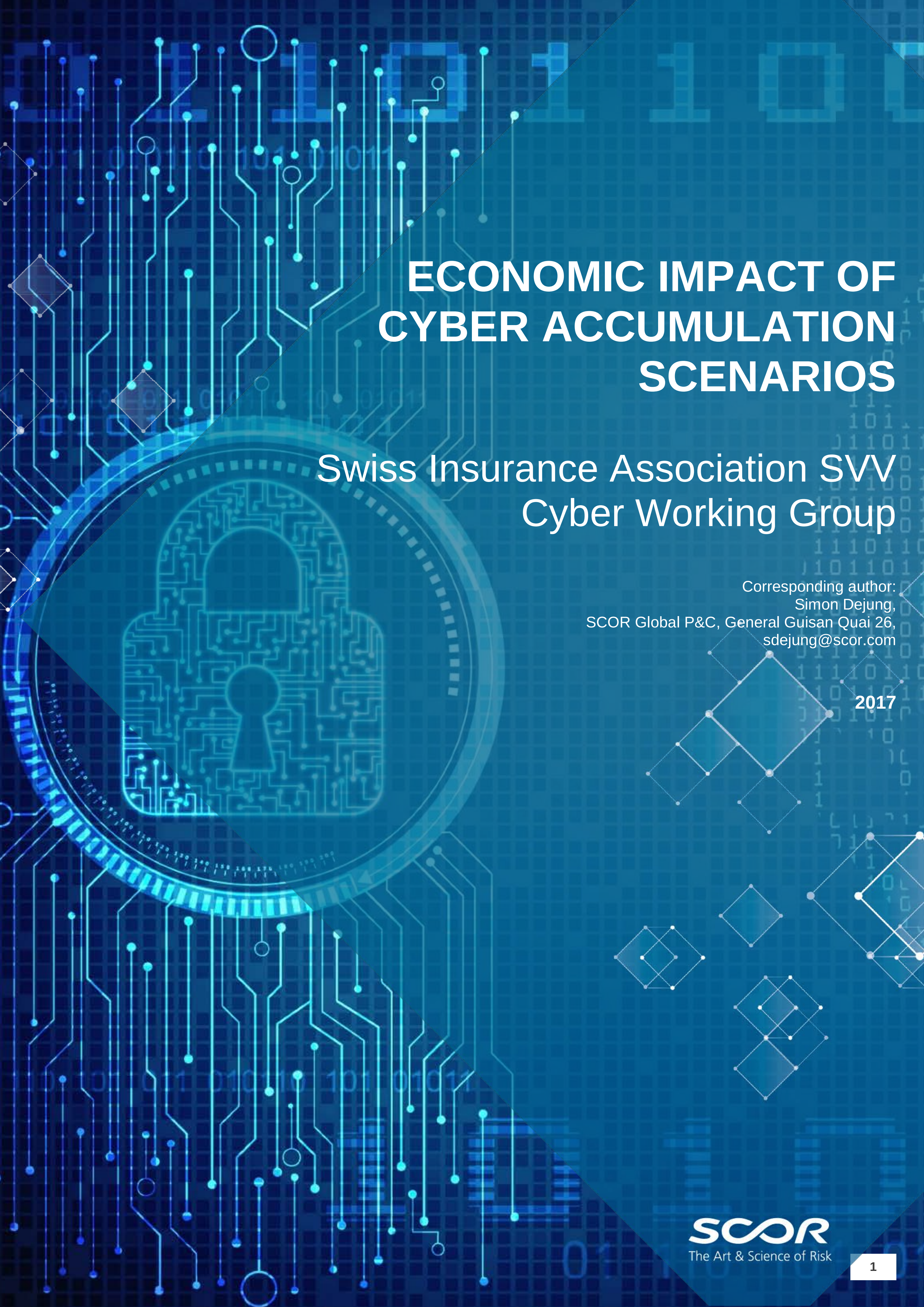

ECONOMIC IMPACT OF CYBER ACCUMULATION SCENARIOS

Swiss Insurance Association SVV
Cyber Working Group

Corresponding author:
Simon Dejung,
SCOR Global P&C, General Guisan Quai 26,
sdejung@scor.com

2017

SCOR
The Art & Science of Risk

TABLE OF CONTENTS

Acknowledgment

THE FOLLOWING EXPERTS AND ORGANIZATIONS – IN ALPHABETIC ORDER, SUPPORTED THIS STUDY. WE ARE VERY GRATEFUL FOR THEIR CONTRIBUTION:

Alexander Odenthal, Raiffeisen
Alexander Schmidl, Munich Re
Andres Rosero, Scor
Angelika Bischoff, Federal Office for Civil Protection
Arie Malz, ISSS
Bernhard Hämmerli, HSLU
Candid Wüest, Symantec
Christian Marx, Scor
Daniel Caduff, Federal Office for National Economic Supply
Daniel Theben, Scor
Dominik Rüfenacht, Swissgrid
Eric Durand, Swiss Re
Fulvio Elia, Axa-Winterthur
Giorgio Ravioli, Federal Office for Civil Protection
Heidi Anneliese Strauss, Munich Re
Ingo Herbst, Siemens
Johannes Steffl, Hannover Re
Linus Neumann,
Lukas Ruf, Consecom
Maher Kamal-Rizk, Scor
Marc Henauer, MELANI
Marc Ruef, Scip
Martin Darms, Darms Engineering
Martin Eling, UNISG
Martin Leuthold, Switch
Michael Hammer, Scor
Oliver Lamberty, Deutscherueck
Peter Burkhardt, Allianz
Peter Lorenz, Scor
Philip Hurni, Swiss Re
Roger Etter, Mobi
Roger Halbheer, Accenture
Roger Iles
Serge Droz, Open Systems
Silke Genuit, Accenture
Stefan Weidmann, UPC
Thomas Dullien, Google
Tobias Seitz, Helvetia
Umberto Aannino, ISSS
Gabor Janki, Trans Re

ECONOMIC IMPACT OF
CYBER ACCUMULATION
SCENARIOS

Abstract

By expert judgment, the impact of five cyber accumulation scenarios (cloud, SCADA, hospitals, power grid and telecommunication) on the Swiss economy was analyzed. These scenarios created an economic impact of 0.2% to 2% of the GDP in the year of the event. These results seem plausible in comparison with catastrophic scenarios presented in other studies (e.g., Federal Office for civil Protection and Cambridge Centre for Risk Studies with assessed economic impacts of approx. 1% to 2% of the GDP in the year of the event. An accumulation scenario by DDOS e.g. on a cloud provider, is the most likely, while the economic impact of a power grid accumulation scenario would be the highest. In addition to pure data recovery and business interruption, physical damages including loss of life, have to be expected by our scenarios. Therefore, payouts by silent coverages are very likely but currently not explicitly priced. Cyber accumulation and pandemic events have their global spread in common. Comparison with NatCat losses and pandemic event estimations suggest that the return period, i.e. frequency of cyber events seems to be of bigger concern, than the economic loss per event.

Introduction & Purpose of the document

Insurance industry fears massive financial impacts due to monocultures and oligopolies in soft- and hardware, which can be exploited simultaneously and worldwide and inadvertent programming errors and vulnerabilities or a logic bomb implemented into the code of an IT/OT software resulting in an accumulation of economic losses and outages. The Swiss Insurance Association SVV installed therefore a working group, which analyzed relevant accumulation scenarios and quantified their economic impact. Furthermore, implications for the insurance sector for affirmative and property & casualty covers will be discussed, e.g. the availability of insurance capacity for P&C and affirmative cyber lines of business and the “silent cover” issue. The outcome and recommendations will be communicated in a position paper and will be addressed to the authorities and interested associations.

During two workshops, in May and July 2017, 17 IT security experts and 14 insurers assessed the potential for accumulation of five scenarios restricted to the territory of Switzerland, knowing that cyber scenarios could affect several countries or regions simultaneously.

Just a few days after the first workshop, the “WannaCry” ransomware exploiting a vulnerability in unpatched Microsoft Windows systems and servers and encrypted files of approx. 300’000 computers worldwide extorting in the average approx. $500 each. According to Johannes Steffl from Hannover Re who was in contact with the National Health Service in UK after the attack, 47 locations were affected in the UK, no bodily injuries nor fatalities occurred due to WannaCry. Persistence was 72h with massive impact on day-to-day routine and working processes. According to the Bitcoin Wallet WannaCry website (Bitcoin Wallet WannaCry-wallet, 2017) only $120k extortion were payed globally until June 2017. Assuming a 3-day persistence of the incident and allocation of an average economic benefit of $500/day per computer would result in an aggregated economic loss of $450m. Under conservative assumptions that additional cascading effects on third parties would double this amount, this would generate an estimated economic impact of less than $1bn, which represents less than 0.001% of the global GDP, i.e. $75’000 bn. In contrast, the accumulation scenarios discussed in this study would result in economic impacts, which would be by a factor 200 higher.

According to the Cyber Crime report from the Center for Strategic and International Studies and McAfee (McAfee, 2014) the annual average loss attributed to cyber-crime was 0.5% to 0.8% of the global GDP. The study stated difficulties to find reliable data for several countries - it is worth to mention, that in general, methods and data to assess cyber incident costs were questioned by ENISA in their study “The cost of incidents affecting CIIs” (ENISA, 2016). Again, the scenarios discussed in our study would be less frequent, result in the same economic impact of approx. 0.5% of GDP just out of one single event at a much lower return period.

Method

Assessed scenarios were measured as a percentage of the Swiss GDP - 2016, 100% = CHF 650 bn, i.e CHF 650 x 10^9 - (SECO - State Secretariat for Economic Affairs, 2017).

- Workshop one – May 2017: five interdisciplinary working groups analyzed three primarily agreed scenarios (DDOS, SCADA, hospitals) which seem realistic and relevant and estimated their economic impact
- Workshop two – July 2017: experts came up with their individual scenarios which affect Swisscom or Swissgrid, which were presented and discussed regarding:
    - Actor, motivation, required resources (know-how, time, infrastructure), penetration, persistence, impact on Swiss economy.
- The two workshop lasted ½ day each.

The following steps were assessed:

- Selection of relevant economic sectors prone to be affected
- Penetration rate of a vector / mean in an economic sector
- Persistence and time until recovery of normal operation
- Investment, i.e. the price, economic effort and development costs to achieve a successful attack. These are e.g. investments into experts and IT/OT infrastructure (test environments or labs)
- Limitations:
    - The assessments were conducted by the working groups through the approximation of impacts and dependencies, based on expert judgment.
    - Long-term effects were not assessed in our study.
    - The assumptions are based on current knowledge and technology
    - Likelihood of scenarios were assessed relative one to another. Return periods, i.e. the frequency or probability of a loss with the same impact were not estimated
    - If cyber attacks are designed to create massive and widespread physical damages of e.g. critical infrastructures, the long lead-time of such components will be the limiting factor, which potentially aggravates the scenarios. We consider such scenarios possible but attribute a low probability.
    - Interactions of global or over-regional cyber incidents were not assessed.
    - Potential rebound effects after recovery and substitution of affected victims (by companies avoiding an attack replacing the ones that are down) have not been taken into consideration when estimating the impact on GDP.

  - We assume that losses increase linear depending on the duration of an event.
  - Required know-how to achieve a successful attack were discussed during the workshops and are subject to the experience of our experts

The reference studies for our assessment were all developed at the Centre of Risk Studies at the University of Cambridge. We have chosen a simplified approach of their methods used for:

- Integrated Infrastructure: Cyber Resiliency in Society (Cambridge Centre for Risk Studies, 2016)
- Business Blackout (Cambridge Centre for Risk Studies, 2015)
- Sybil Logic Bomb Cyber Catastrophe (Cambridge Centre for Risk Studies, 2014)

Accumulation scenarios

- Distributed denial of service (DDOS) attack (on a cloud provider)
- Simultaneous attack on industrial control / supervisory control and data acquisition (ICS/SCADA) systems
- Simultaneous broad attack on several hospitals
- Cyber attacks on Switzerland biggest telecommunication provider
- Cyber attacks on Swiss power grid and/or regional power distributers with their substations and/or power producers

Cloud scenarios

DDOS attacks became frequent and are predominantly targeted attacks, with the intention to create interruption and reduce availability of the victim. They can happen repeatedly affecting the same victim several times. In the meantime defense strategies are well developed.

Four teams analyzed DDOS attacks on DNS servers, cloud providers and one studied DDOS impact on financial services and trade.

- 62% of the Swiss GDP over a short period could be affected – most sectors only slightly - by an accumulated cloud attack scenario
- We assume 20 to 30% of the cloud providers to be affected
- Impact on the affected services 90%
- Outages - one day to one week

1/ Actors / Motivation

Criminals with the goal of earning money through extortion. Politically, economically or religiously motivated state sponsored attackers are also possible. Scaling it up to a level of accumulation requires infrastructure and staff.

2/ Required know how and resources of the attackers

Five experienced software engineers. Working for 2 months. This requires an investment of approximately CHF 0.1m.

3/ Economic impact

CHF 0.2 to 1.3 bn, i.e. 0.03% to 0.2% of Swiss GDP, caused mainly by additional cost of working, e.g. system recovery, data restoration and extra hours and only marginal turnover impact due to a rebound effect after recovery.

SCADA/ICS scenarios

Automation market leader is SIEMENS with estimated 30% to 40% market share. State of the art SCADA/ICS standard protocols allow integration and plug and play of different vendors and consequently different manufacturer can be present in one production plant sharing that way certain vulnerabilities. We have therefore chosen two different scenarios where countrywide 10% - which we consider a low penetration - of the SCADA/ICS system were compromised or shut down for precaution measures. Persistence 3 weeks.

Figure 1 shows ICS systems in Switzerland, connected to the internet mid-April 2017, with the following widely used protocols, s7, modbus, fox, dnp3, bacnet. The figure was provided by *Freie Universität Berlin, AG Sichere Identität / SCADACS*. They used their censys.io search engine.

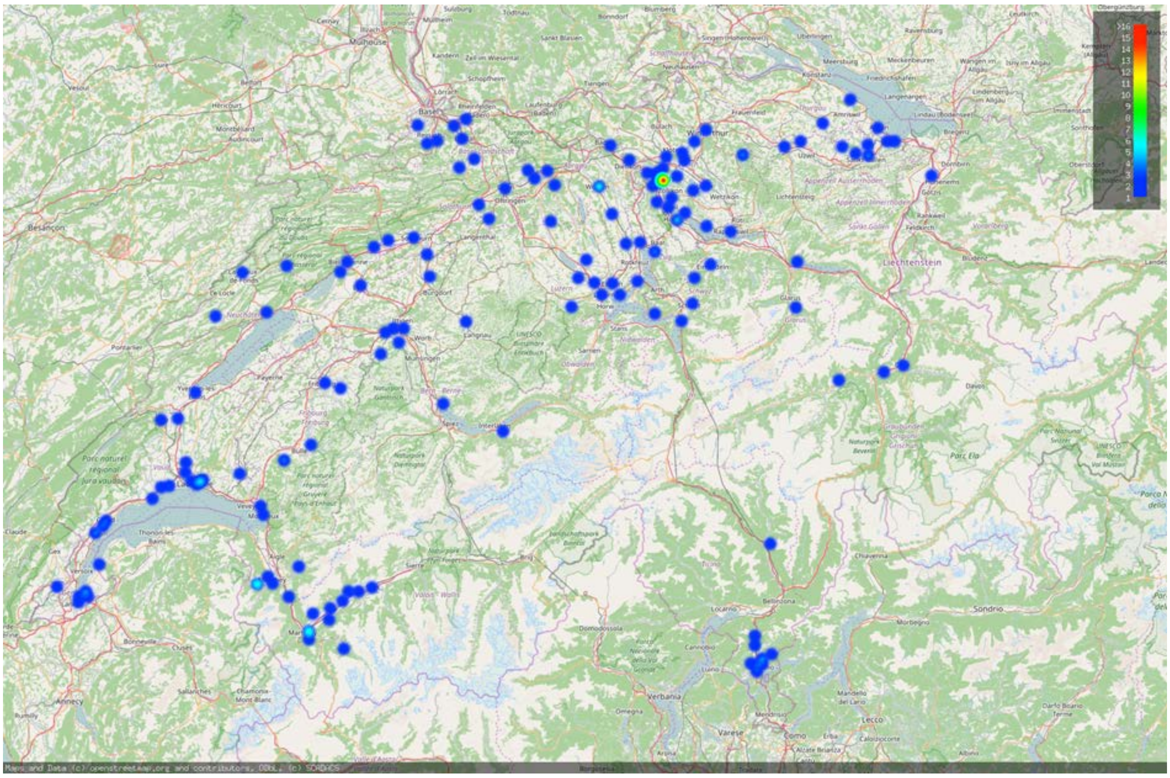

Figure 1: ICS systems in Switzerland, connected to internet mid-April 2017(protocols, s7, modbus, fox, dnp3, bacnet)

1/ Scenario 1 – Industroyer/Crashoverride derivate

Industroyer/CrashOverride from July (US-CERT, 2017) derivate. Penetration of the scenario differs in an affected industry sector. We see the following sectors to be mainly affected:

- Manufacturing / production
- Energy
- Traffic
- Water supply
- Health
- Agriculture
- Construction

1 - 1. Actors/Motivation

Politically, economically or religiously motivated state sponsored attackers.

1 - 2. Required know how and resources of the attackers

Accumulation scenario 1 is complex in design and execution, needs know how, infrastructure and workforce, reason why we attribute it to state affiliated actors or high sophisticated terrorists or criminals. We assume that a team of at least five up to 20 IT/OT security experts, hackers and process specialists over a period of four months to a year are required to prepare such an attack. They often start with a multi-stage attack procedure over several attack vectors e.g. spear phishing and social engineering with the aim to obtain IT/OT credentials and high authority level. A (threatened) insider would reduce required preparation time and resources for such an attack and increases the prospect of success. In addition, a test environment would increase the likelihood of a successful attack but would presuppose at the same time infrastructure investments of up to CHF 10m.

2/ Scenario 2 – Modification of process variables

To contrast this, we went through a targeted SCADA/ICS extortion scenario, where simple process variables were maliciously modified to change the product properties. The victims are important pharmaceutical or food producers. They are blackmailed, e.g. Friday evening with the information, that their fabrication was modified already a while ago. To learn the time of initial deployment and to get knowledge of the variables compromised they have to pay a ransom until Monday. If they do not, the criminals threaten to deploy the attack to other subsidiaries of the group. In addition, the attackers move from one manufacturer to the next simultaneously. To prove their capabilities they create a spillover in a sewage treatment plant. The vulnerability gets public and starts to worry the society. The leaked zero-day motivates freeloaders to copy and amplify the attack and increase its footprint.

2 - 1. Actors/Motivation

Scenario 2 is less complex. Actors are cyber criminals potentially supported by (threatened) insiders / Ransom.

2 - 2. Required know how and resources of the attackers

Process know how, remote (support) access to the ICS system of an installation. Six months lead time for investigation and preparation. Investment < CHF 200k.

3/ Economic impact scenarios 1 & 2

The annual GDP contribution of affected sectors are CHF 150 bn to 370 bn, depending on assumed penetration of the two scenarios per sector. The persistence of the two scenarios of 3 weeks resulted in an economic impact between CHF 0.3 bn to 2.2 bn, i.e. 0.05% to 0.3% of Swiss GDP caused mainly by business interruption and loss of profit, additional cost of working, physical damages including accidents and fatalities. We consider the accumulation potential of scenario 2 lower but potentially more frequent with a higher chance to monetize the attack.

4/ Limitations

If SCADA/ICS attacks not only affects the IT/OT but instead would be designed to create massive physical damages, e.g. a derivative from STUXNET and destroy many components at the same time, their long lead-time might potentially aggravates the scenarios. We consider such scenarios possible but attribute a low probability. In addition, cascading and long-term effects were not assessed systematically.

Health sector & hospitals scenario

A sophisticated cyber-attack infiltrates several Swiss hospitals and becomes active at the same time - either as Ransomware and / or DDOS - with the result that the hospitals are not available for 2-3 weeks. Neuss hospital, Germany as a reference took about 3 weeks to come back in operation. The damage in Neuss amounted to approx. EUR 1 million (restoration costs, external IT specialists, turnover). However, according to LKA, it was no targeted cyber-attack.

1/ Actors / Motivation

Politically or economically motivated state sponsored attackers. An accumulation scenario is complex in design and execution and needs know how, infrastructure and workforce, reason why we attribute it to state affiliated actors or high sophisticated terrorists or criminals.

2/ Required know how and resources of the attackers

Five experienced software engineers. Required time for preparation, research and tests: 6 months. This requires an investment of approximately CHF 0.5m.

3/ Economic impact

Business interruption and loss of profit, additional cost of working, physical damages including accidents and fatalities.

Income of 288 Swiss hospitals in 2015 was CHF 24 bn (Federal Office of Public Health FOPH , 2015).

- 3 weeks total outage of all hospitals: 1.4 bn CHF, i.e. 0.2% of Swiss GDP
- 3 weeks total outage 10% of the hospitals: 138 m CHF
- 1 week Total loss 10% of the hospitals: 46 million CHF

3/ Comment

Many hospitals have a lot of soft- and hardware in common. Nevertheless, architecture, implementation and configuration are individual and the likelihood of successful accumulation scenarios affecting more than 10% of the Swiss hospitals have a low to medium likelihood.

Power grid & power providers scenarios

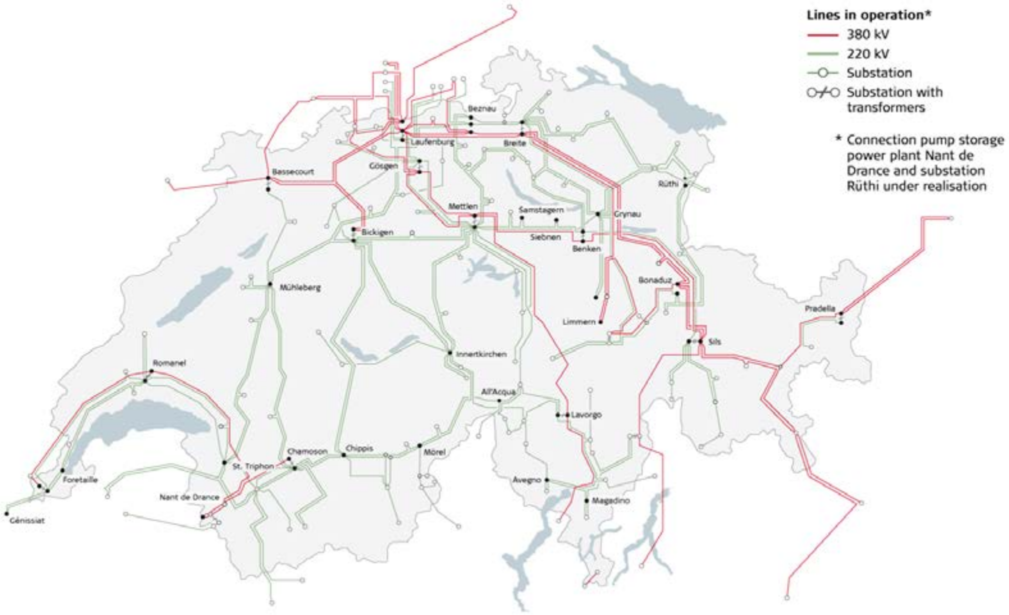

Figure 2 : Swiss 380 & 220 kV grid and substations (www.swissgrid.ch)

This scenario was inspired by and the cyber induced Ukrainian power outages in December 2016 (E-ISAC / SANS, 2016), where the INDUSTROYER / CRASHOVERRIDE ICS malware was deployed in order to attack multiple electricity substations, switches and circuit breakers, turning off power distribution and triggering a cascade of failures and damaged equipment (dragos.com, 2017). Functionalities of this malware were analyzed among others by ESET (ESET, 2017).

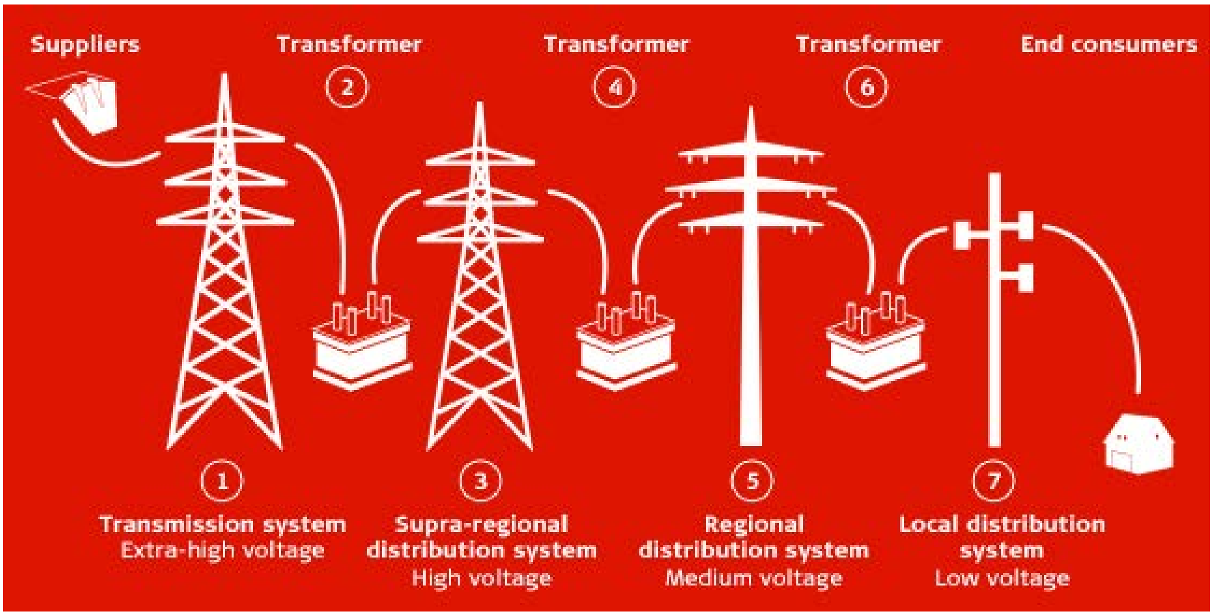

Figure 3: Swiss power grid is divided into seven grid levels and three transformation levels (www.swissgrid.ch)

1/ Actors / Motivation

Politically, economically or religiously motivated state sponsored attackers. Criminals are less likely but possible.

2/ Required know how and resources of the attackers

This depends on the targeted power infrastructure; see figure 3 – generation, transmission (TNO) and/or distribution (DNO) - and targeted impact – local, regional or countrywide. We assume that a team of at least five up to 20 IT/OT security experts, hackers and power grid specialists over a period of four months to a year are required to prepare such an attack. They often start with a multi-stage attack procedure over several attack vectors e.g. spear phishing and social engineering with the aim to obtain IT/OT credentials and a high authority level - see therefore the following security awareness video “Anatomy of an ICS Network Attack” (SANS, 2016). A (threatened) insider would reduce required preparation time and resources for such an attack and increases the prospect of success. In addition, a test environment would increase the likelihood of a successful attack but would presuppose at the same time infrastructure investments of up to CHF 10m.

3/ Persistence

The attack has the potential to persist two to seven days at 100% intensity. After two days the characteristics of the attack are understood and countermeasures are carried out which bring gradually back electricity. Depending on the magnitude of the attack, full recovery of the power infrastructure is expected after five to 21 days, which corresponds to the S1 and the S2 scenarios of the Lloyd’s / Cambridge Business Blackout (Cambridge Centre for Risk Studies, 2015).

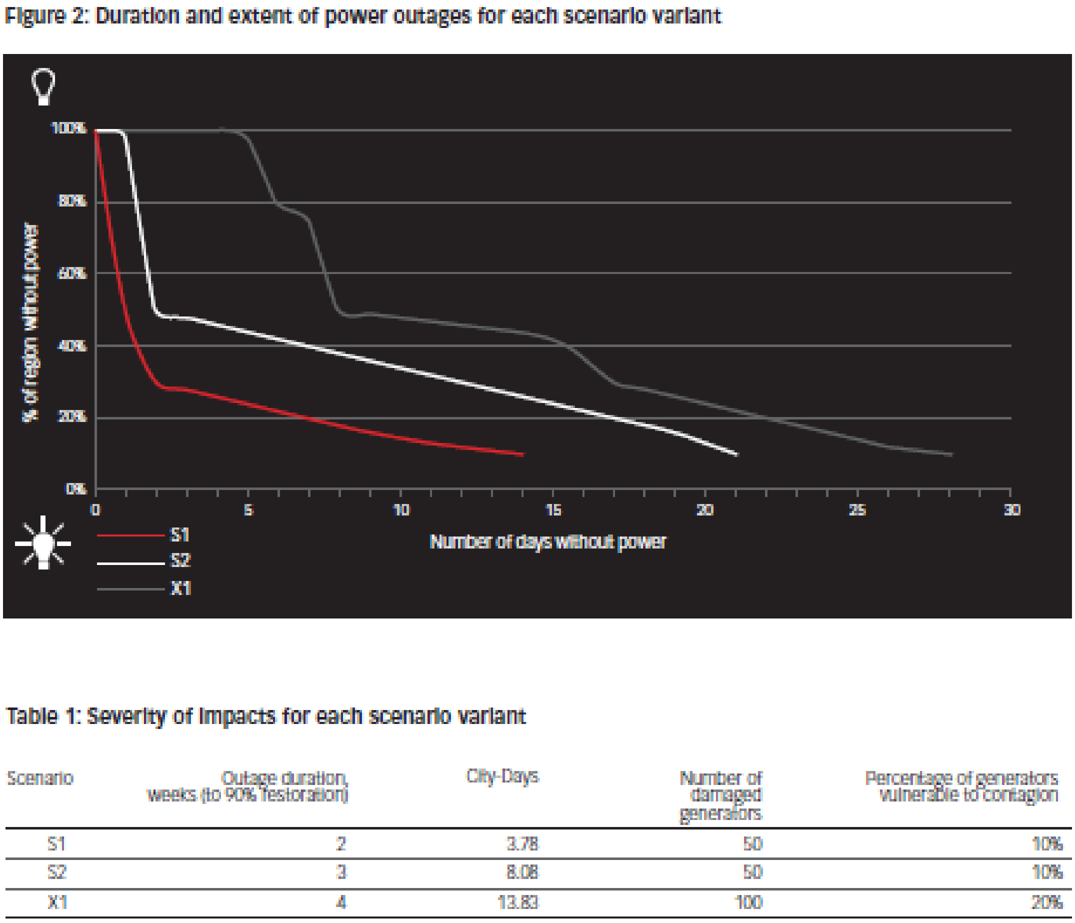

Table 1: Severity of impacts for each scenario variant

Scenario	Outage duration, weeks (to 90% restoration)	City-Days	Number of damaged generators	Percentage of generators vulnerable to contagion
S1	2	3.78	50	10%
S2	3	8.08	50	10%
X1	4	13.83	100	20%

Figure 4: Duration and extent of power outages

4/ Economic impact

We estimate, based on a conservative approach, an economic impact of 80% to 100% on the Swiss GDP for two to seven days of attack persistence. We considered scenarios for economic centers like Zurich and scenarios paralyzing the entire country. The city of Zurich contributes with 11%, the canton of Zurich contribute with 22% to the Swiss GDP. We give therefor a range of CHF 300m to 12bn economic impact, which corresponds to <0.01% up to 2% of the Swiss GDP.

5/ Limitations

Within our working group, the downtime assumptions and time until complete recovery - i.e. several days to several weeks - diverged the most for the power scenarios. This is mainly due to the fact, that SCADA/ICS malware (e.g. Industroyer, Stuxnet, Blackenergy, Dragonfly, etc.) could not only affect the IT/OT, but instead could be designed to create massive physical damages in many generators or transformers or destroy control units at the same time. The long lead-time of such components will be the limiting factor, which potentially aggravates the scenarios. We consider such scenarios possible but attribute a low probability. In addition, cascading and long-term effects were not assessed systematically.

Telecommunication scenarios

1/ Scenario 1 – Router or modem zero-day

A sophisticated zero-day malware targets e.g. a router or modem with 50% market share. As the IP addressed are known prior to the attack, the infection rate reaches 95% within 30 minutes. The malware deletes the firmware and the devices have to be replaced impacting internet connectivity and telecommunication of 75% of the device end-users. The stock for such a device covers only 10% of the demand and only after two weeks, the routers can be delivered and replaced. Consequently, affected users change after three days for other devices, but this leads also there to a supply bottleneck of ten days. The productivity is halved during this time.

1 - 1. Actors/Motivation

Criminals or politically, economically or religiously motivated state sponsored attackers.

1 - 2. Required know how and resources of the attackers

Five experienced software engineers specialized in reversing and firmware analysis. Working for 3 months (find or buy exploit, test attack). This requires an investment of approximately CHF 0.5m. A Border Gateway Protocol (BGP) attack might require less know how and has to be expected more frequently.

1 - 3. Economic impact

We assume an attack persistence of seven days, which affects during this period 18% (0.5*0.95*0.75*0.5) of the Swiss GDP resulting in a 2.25bn economic impact, i.e. 0.35% of Swiss GDP. The impact and severity of potentially more frequent BGP attacks should be lower due to shorter persistence of the attack.

2/ Scenario 2 – Domain name servers

A Distributed Denial of Service (DDoS) attack on main DNS providers using a botnet. The botnet consists of millions of malware infected internet-enabled devices (IoT) where the criminals take advantage of the low security standards. At a busy Internet shopping day, e.g. Christmastime, the criminals start the attack. Unavailability 1 day.

2 - 1. Actors/Motivation

Criminals with the goal of earning money through extortion. Politically, economically or religiously motivated state sponsored attackers are also possible.

2 - 2. Required know how and resources of the attackers

Five experienced software engineers. Working for 2 months. This requires an investment of approximately CHF 0.1m.

2 - 3. Economic impact

ICT dependent economic sectors and online business (B2B and B2C) will slow down and result in a loss of CHF 200m, i.e. 0.03% of the Swiss GDP.

3/ Scenario 3 – Cryptolocker paralyzes Swisscom

Unavailability 2.5 days.

3 - 1. Actors/Motivation

Politically, economically or religiously motivated state sponsored attackers

3 - 2. Required know how and resources of the attackers

Five experienced software engineers create a WannaCry / Petya / NonPety derivate. Required time for preparation, research and tests: 6 months. This requires an investment of approximately CHF 0.5m.

3 - 3. Economic impact

Massive impact on Swiss economy for 2.5 days reducing the productivity to 50%. This results in a loss of CHF 2.5bn, i.e. 0.4% of the Swiss GDP.

Insurance Considerations

The assessed accumulation scenarios of the previous sections might not only have an impact on IT systems and data, but also have an impact on physical and financial assets. Some could endanger life and disrupt or interrupt economic processes, leading to cascading effects and impacting third parties. Beside affirmative cyber coverages, some scenarios might "silently" trigger several other insurance lines of business due to unclear, inappropriate or outdated wordings creating contract uncertainty (IMIA Working Group 98, 2016). One obvious example are acts of cyber war and terror, for which IT forensics will hardly be able to clearly distinguish from cyber-crime, making it difficult to invoke the war or terror exclusions. Moreover, the policyholder might reject the insurance decision and appeal to a court, thus creating even more uncertainty.

In most cases, the lack of power supply or unavailability of telecommunication would not trigger indemnification for the policy type predominantly used by SMEs because it typically provides cover based on named perils and/or with a clear physical property damage trigger.

On the other hand “all risk” policies - i.e. most technical insurance lines and property policies for big corporates and multinationals – if not clearly excluding the perils of power outage or unavailability of telecommunication – might indemnify ensuing physical damages (PD) and consequential business interruption / loss of profit (BI/LOP). An example of a covered loss for technical and P&C extensions is the deterioration of stock, e.g. food or medicine, due to the interruption of the cold chain.

Business interruption / loss of profit P&C coverages without a PD trigger are not standard; however, unfortunately they become increasingly common. Presumably, these policies cover also losses as a consequence of a cyber incident, i.e. unavailability of ICT soft- and hardware. If the cyber exposure is not clearly addressed in the terms and conditions of the policy, we have to assume a cyber coverage where no premium was charged.

We assessed the economic impact of accumulation cyber scenarios on a level of less than 2% of the Swiss GDP, whereas the majority of the scenarios create an impact below 0.5% of the Swiss GDP. It seems plausible that the Swiss economy would not be brought down by such scenarios, but that many SMEs and corporates would not have any or enough insurance cover, possibly creating the need for an emergency state intervention to prevent the collapse of these multiple companies. In addition, state owned services and large corporates tend to self-insure, resulting in a considerable amount of uninsured economic losses.

A further concern for the insurance industry is the fact that silent cyber exposure is often not priced for in the regular line of business covers – often due to ambiguous policy wordings and to the not understood frequency question - but indemnification still might be triggered for some of the covers, possibly after long legal disputes.   This also means that policy holders cannot rely on indemnification due to potential silent covers. See also the UK regulators consultation paper CP39/16 regarding silent cyber coverage, where in addition the capital underlying the capacities has to be questioned (Bank of England - Prudential Regulation Authority, 2016). This ambiguity creates a combined responsibility of the already insureds and potential insureds, but also from the insurance industry, to create clarity in the policy wordings taking into account new realities and worded appropriately - a clearly worded example fit for purpose for all property and casualty lines is the recently released IMIA cyber exclusion with write-back option (IMIA, 2017). On the other hand, policy buyers have to make sure that when purchasing insurance their cyber exposure is addressed adequately, avoiding ambiguities.

Investment, likelihood & impact of an accumulation scenario

We asked the experts to rank the likelihood of a scenario and estimate required investments of the attackers to achieve maximum economic and BI impact:

Table 1: Descending likelihood, coverages triggered & economic consequences of an accumulation scenario

Accumulation Scenario	**Likelihood ranking (descending)**	**Max. Swiss GDP impact**	**Time estimation until 100% recovery**	**Investment [m CHF] for max. impact**	**Covered by affirmative cyber**	**Covered (partially) by P&C**	**CBI and/or service provider**
CLOUD	1	0.2%	7 days	0.1	Yes	No	No
HOSPITALS	2	0.2%	21 days	0.5	Yes	Yes	No
TELECOMM	3	0.7%	10 days	0.5	Yes	No	No
SCADA/ICS	3	0.3%	21 days	10	Yes	Yes	No
POWER GRID	4	2%	21 days	10	No	Yes	Yes

Comparison with NatCat scenarios

Economic and insurance losses caused by NatCat, which are spatially limited and pandemic events, which can have a global spread, are better understood by the society and the insurance industry than the impact of widespread cyber events. Cyber accumulation scenarios have to be put into the same context to get a better understanding for potential economic impacts in relation to the GDP of a country, region, continent or worldwide. According to our assessments, the presented cyber accumulation scenarios would affect the economy less, than a massive NatCat event, e.g. massive earthquakes or a pandemic scenario. Historic data allow estimations of return period of catastrophic events. For cyber, this is not the case and the unknown frequency is of major concern.

Table 2: Economic & insurance losses of NatCat & pandemic events

Event (with links for further information)	**Impacted Countries**	**Economic Loss estimation [bn CHF]**	**Max. GDP impact on affected countries**	**Insurance Loss estimation [bn CHF]**
Basel earthquake, 1356 as at today	CH	100	15%	10
Thai Floods, 2011	TH	43	10%	16
Japan earthquake, tsunami, 2011	JAP	210	5%	40
Pandemic scenarios CH	CH	14.5	2.2%	n.a.
Pandemic scenario US	US	n.a.	5%	n.a.
Pandemic scenario UK	UK	70	4%	n.a.
Pandemic scenarios EU-25	Europe	n.a.	4%	n.a.
Zurich Flood worst case scenario	CHF	5.5	0.9%	n.a.
Hurricane Katrina, storm surge, 2005	USA	125	0.7%	61
Sandy superstorm, 2012	USA	70	0.4%	30
Lothar/Martin Winterstorm Dec, 1999	Europe	15	0.1%	9
European Flood 2002	Europe	15	0.1%	4
European Flood 2013	Europe	15	0.1%	4
Hailstorm Reutlingen 2013	D	4	0.1%	3

Extreme scenarios & price of successful widespread attacks

According to Costin Raiu from Kaspersky Lab, the development costs of STUXNET are estimated on a level of $100m and were attributed to Israel and the USA. Although a zero-day exploit on an individual ICS/SCADA system can be purchased for less than $10k according to www.gleg.net CEO Yuriy Gurkin (Paganini, 2015), a successful, coordinated wide-scale cyber-attack remains very complex and costly. We assume that development, testing and deployment of INDUSTROYER-like malware today would require approximately a $10m investment, which is ten times less than estimated for STUXNET. The attractiveness for criminals to finance such attacks can be questioned, as it is difficult to monetize them compared to ransomware or DDOS.

Our expert team attributed successful widespread attacks on ICS/SCADA systems, the power grid or the telecommunication systems mainly to state affiliated actors. A minority came up with scenarios executed by criminals. We therefore assume that high severity losses with high persistence and penetration - which define the accumulation potential - are complex and more likely to be state sponsored, while high frequent, low severity losses with accumulation potential e.g. DDOS or Ransomware could origin from both, criminals and state sponsored actors. Targeted extreme scenarios with high severity potential like attack on the Sihlsee hydro power dam upstream the river Sihl, 35km from Zurich, or a nuclear power plant are out of scope and were not assessed in this study. We believe that such scenarios have a clear warlike character, are extremely complex and difficult to succeed, knowing that there is no clear demarcation between cyber-crime and cyber war.

Conclusion

We were interested in the order of magnitude of cyber accumulation scenarios and assessed their impact on the GDP and we tried to assess the likelihood of an accumulation scenario relative to one another. All accumulation scenarios created economic impacts of 0.2% to 2% of the annual GDP. They withstand plausibility checks with the catastrophic scenarios of the Federal Office for civil Protection (Federal Office for civil Protection FOCP, 2015). Their comparable scenarios (power supply, ICT, cyber-attack) result in economic impacts of approx. 1% of the Swiss GDP. The same is valid for the studies conducted at the Cambridge Centre for Risk Studies, where the economic impact of logic bombs and power blackouts were analyzed. An important problem is that this type of cyber exposures are not priced for, partly because return periods (i.e. frequencies) of cyber accumulation events are not understood - as they are man-made, they depend on many factors which can variate over times and partly because cover is not transparently granted.

Bibliography

Bank of England - Prudential Regulation Authority. (2016). *Cyber insurance underwriting risk.* Retrieved from Cyber insurance underwriting risk: http://www.bankofengland.co.uk/pra/Documents/publications/cp/2016/cp3916.pdf

Bitcoin Wallet WannaCry-wallet. (2017). *bit info charts*. Retrieved from https://bitinfocharts.com/bitcoin/wallet/WannaCry-wallet

Cambridge Centre for Risk Studies. (2014). *Sybil Logic Bomb Cyber Catastrophe*. Retrieved from http://cambridgeriskframework.com/page/25.

Cambridge Centre for Risk Studies. (2015). *Business Blackout*. Retrieved from http://cambridgeriskframework.com/page/20.

Cambridge Centre for Risk Studies. (2016). *Integrated Infrastructure: Cyber Resiliency in Society*. Retrieved from http://cambridgeriskframework.com/page/20.

dragos.com. (2017). Retrieved from CRASHOVERRIDE Analysis of the Threat to Electric Grid Operations: https://dragos.com/blog/crashoverride/CrashOverride-01.pdf

E-ISAC / SANS. (2016, March 18). Retrieved from Analysis of the Cyber Attack on the Ukrainian Power Grid: https://ics.sans.org/media/E-ISAC_SANS_Ukraine_DUC_5.pdf

ENISA. (2016). *The cost of incidents affecting CIIs* . Retrieved from https://www.enisa.europa.eu/publications/the-cost-of-incidents-affecting-ciis/

ESET. (2017, June 12). Retrieved from Industroyer: Biggest threat to industrial control systems since Stuxnet: https://www.welivesecurity.com/2017/06/12/industroyer-biggest-threat-industrial-control-systems-since-stuxnet/

Federal Office for civil Protection FOCP. (2015). *Disasters and Emergencies in Switzerland*. Retrieved from http://www.babs.admin.ch/de/aufgabenbabs/gefaehrdrisiken/natgefaehrdanalyse/gefaehrddossier.html

Federal Office of Public Health FOPH . (2015). *Key figures for Swiss hospitals*. Retrieved from https://www.bag.admin.ch/bag/de/home/service/zahlen-fakten/zahlen-fakten-zu-spitaelern/kennzahlen-der-schweizer-spitaeler.html

IMIA. (2017). *Endorsement – IMIA Advanced Cyber Exclusion 2017.* Retrieved from Endorsement – IMIA Advanced Cyber Exclusion 2017: https://www.imia.com/wp-content/uploads/2017/03/Endorsement-IMIA-Advanced-Cyber-Exclusion-2017-final-15-03-2017.pdf

IMIA Working Group 98. (2016). *Cyber Risks - Engineering Insurers Perspective*. Retrieved from https://www.imia.com/wp-content/uploads/2016/09/IMIA-Working-Group-Paper-9816-Cyber-Risks-Rev-A002-16-09-20161.pdf

JLT Re. (2017). *VIEWPOINT - Unlocking the potential of the cyber market.* Retrieved from VIEWPOINT - Unlocking the potential of the cyber market: https://www.jltre.com/~/media/files/sites/jltre/insights/viewpoint/jlt_re_viewpoint_cyber_april_2017.pdf?la=en-gb

McAfee. (2014). Retrieved from Net Losses: Estimating the Global Cost of Cybercrime: https://www.mcafee.com/us/resources/reports/rp-economic-impact-cybercrime2.pdf

Paganini, P. (2015). *http://securityaffairs.co/wordpress/41385/cyber-crime/scada-zero-day-exploit-cost.html*. Retrieved from http://securityaffairs.co/wordpress/41385/cyber-crime/scada-zero-day-exploit-cost.html

SANS. (2016, March 25). Retrieved from SANS Securing The Human: https://www.youtube.com/watch?v=_eNB1gq5gbA&index=3&t=7s&list=PLQd41Go4Yv49I0xbEjPlx_qxwbIrlDPOh

SECO - State Secretariat for Economic Affairs. (2017). Retrieved from Gross domestic product quarterly data: https://www.seco.admin.ch/seco/en/home/wirtschaftslage---wirtschaftspolitik/Wirtschaftslage/bip-quartalsschaetzungen-/daten.html

US-CERT. (2017, July 7). Retrieved from CrashOverride Malware: https://www.us-cert.gov/ncas/alerts/TA17-163A

Yuriy Gurkin. (n.d.). Retrieved from http://www.gleg.net/agora_scada.shtml