Research Fund

Building Cyber Resilience

Threats, Enablers and Anticipation

A collection of perspectives by the AXA Research Fund

Winter 2021

About the AXA Research Fund

The AXA Research Fund was launched in 2008 to address the major risks faced by our planet. AXA has committed a total of €250M to scientific philanthropy and supported 665 research projects in key risk areas of health, climate and environment and socio-economics. The AXA Research Fund's philanthropic mission is to fund and support transformative scientific research and to help inform science-based decision-making in both the public and private sectors through dissemination activities.

www.axa-research.org

@AXAResearchFund

axaresearchfund@axa.com

Contents

About the AXA Research Fund 2

Foreword 3

Executive Summary 4

Security and Privacy: Friends or Foe? 8

- The Double-Edged Sword of Cyber Security 10
- Privacy and Accountability Need Not Be Opposing Goals 12

Mitigating Cyber Risk – from Critical Infrastructures to Quantum 14

- Designing and Retrofitting Resilience into Critical Infrastructures 16
- New Strategies to Enhance Cyber Security in the Cloud 18
- AI and Machine Learning: Defense Mechanisms That Need to Be Defended 20
- Quantum: An Additional Threat? 22

Cyber Resilience of Organizations and States 24

- Building Cyber-Resilient Organizations 26
- Cyber Resilience in the Post-Pandemic World — An Urgent Need for Data-Sharing and Co-Operation 28
- Cyber Ecosystems against Cyber-Crime 30
- Organizing and Regulating Cyber Space 32

Insuring Cyber Risk – a Shift in Paradigm 36

- The Challenges of Cyber Risk Insurance 38
- A Shift in Risk-Modelling Techniques for Connected and Autonomous Vehicles 40
- Accumulation, Dependence and Extreme Scenario Building: Preconditions for Cyber Risk Insurability 42

Future Scenarios and Trends 44

- Strategic Foresight and Sci-Fi to Help Better Understand Future Threats 46
- Anticipating the Future of Cyber-Attacks: Tales from the Future and Real-Life Points of Caution 48
- Around the World in Future Cyber Trends 52

Foreword

While cyber space provides major opportunities for innovation, economic progress, and access to information, it also entails new vulnerabilities. In fact, cyber-attack volumes are growing every year with increasingly stunning operations, moving from personal data breaches attacks on critical infrastructures such as pipelines, water reservoirs and even health systems. The cost of cyber-crime damage is increasing at a surprisingly rapid pace every year. Vulnerabilities are compounded by the growing interconnectivity of everything around us, making attacks easier to conduct with an array of objectives that make them harder to counter. Cyber security has become everyone's problem.

Cyber-crime is now firmly established as a sophisticated shadow industry, as evidenced by the offering of "ransomware-as-a-service".[1] Some cryptocurrencies can foster stealth flows of money extorted through cyber hacks. This is compounded by cyber warfare and nation state sponsorship. Beyond the anonymity of the perpetrators, the blurred chain of command, influence and pre-funding raises the question of the qualification of some attacks as acts of war.

Cyber risk is among the most pressing and quickly morphing risks for society and for insurers. Cyber risk raises insurability challenges because its systemic nature undermines the principles of pooling and diversification that lie at the heart of the insurance business. As large-scale global organizations, insurers themselves can also be prime targets for cyber criminals.

The 2021 AXA Future Risk Report[2] found that experts view cyber the #2 top risk, second only to climate change. In this context, better understanding and estimating cyber risks is crucial to help develop informed strategies that consider the interconnectivity of our systems and the possible cascading consequences of a cyber-attack. These strategies need to couple prevention with resilience to damage.

With this report, the AXA Research Fund brings together academic, business and organizational expertise to highlight the changing dynamics of the cyber landscape and to contribute to the understanding towards the mitigation of the associated risks and, in doing so, protect what matters.

Marie Bogataj

Head of the AXA Research Fund and Group Foresight.

Renaud Guidée

Group Chief Risk Officer at AXA and Chairman of Net-Zero Insurance Alliance.

[1] The Destructive Rise of Ransomware-As-A-Service, Barbara Kay, Forbes, June 9, 2021
[2] 2021 AXA Future Risk Report, AXA, September 2021

Executive Summary

Since the onset of the Covid-19 crisis, there has been a visible surge in cyber-attacks, phishing scams and malicious activity targeting critical infrastructures, governments, organizations and end-users. In 2020, cyber-attack statistics increased dramatically with a 300% surge in cyber-crime events in the US,[1] a 600%[2] increase in malicious emails worldwide just a few months into the crisis and a 70%[3] rise in healthcare industry data breaches over the previous year.

The health crisis has brought about behavioral shifts that will persist long after the pandemic in every area of our lives — the standard adoption of remote working and a shift to online transactions in almost every realm including healthcare consultations, shopping and banking — making the available "cyber-attack opportunity pie" far larger than ever before. At the same time, digital attacks have become more sophisticated and the threat environment more complex.

Organizations must simultaneously sift through alerts, track vulnerabilities, apply security policies across various systems and endpoints, and accurately assess threat data in real time. Given the complexity of the task, organizations are changing their security posture from a defensive stance to a more realistic and resilient approach.

Cyber resilience actively monitors and builds defense systems in advance to respond to risks, threats, and vulnerabilities. A cyber-resilient strategy helps an organization protect itself against cyber risks and ensures its continued survival in the face of an attack. It is an approach that relies on research and novel techniques for defense but also on collaboration between organizations and even nation states, with a crucial role for regulation.

As one of the top three global risks highlighted by the AXA 2021 Future Risk Report,[4] cyber risk clearly requires preparedness. It is a challenging field as the lack of historical data, the constantly evolving threat profile and issues of clustering and correlation of cyber events require new strategies, techniques, and policies towards mitigation.

In this publication, the AXA Research Fund brings together 20 expert contributors from academia, governmental and international organizations as well as the insurance industry to inform around the key question of building cyber resilience.

[1] FBI Official Warns of Increasing Cybercrime Attacks Related to Coronavirus-Relief Efforts, The Washington Times, April 2020
[2] The Latest: UN Warns Cybercrime on Rise During Pandemic, The Associated Press, ABC News, May 2020
[3] 2020 Data Breach Investigations Report, Verizon, 2020
[4] 2021 AXA Future Risk Report, AXA, September 2021

Key Learnings

In the digital world, privacy often seems at odds with security and accountability, but that does not have to be the case.

Malevolent activities in cyber space are countered by using AI solutions that are often invasive and seem to compromise the societal values that cyber technologies were meant to serve. However, in the long term, the development of experimental proof of personhood methods that create anonymous-but-accountable digital tokens could securely and uniquely represent real people without having to identify them. These approaches promise strong security and accountability with full digital and physical anonymity, meaning that both privacy and security may well be ensured in parallel.

While new technologies can increase the opportunities for cyber-attacks, techniques for managing cyber risk are emerging from both traditional infrastructure systems and new technologies themselves.

Cyber risk is possibly most visible when applied to critical infrastructure systems – the most telling illustration of the impact of the digital world on the physical. In this area, building resilience against cyber risk relies on "resilience by design" techniques that integrate the potential of an attack within the operation of a system and provide buffers, flexible sourcing options or temporary built-in disconnection from the network to continue providing critical production in case of an attack.

In addition to physical resilience building techniques, **the new fields of 'adversarial machine learning' and 'adversarial risk analysis' are emerging to make machine learning systems robust against malicious attacks**. Forecasting, attacker behavior and asymmetries in information between attacker and defender are at the heart of this resilience approach to build stronger defense mechanisms.

Virtualization in the cloud provides more opportunities for attack compared to proprietary systems as it provides a larger 'attack surface' than on-premises information systems — in the machines themselves, the service provider side, or the user side. **This has triggered the development of adapted strategies such as "Zero Trust"** that ensure the creation of secure spaces separated by gatekeepers (e.g. firewalls) between an application server and a database server, **digital multi-level security layers or 'least privilege' principles** that apply processes which grant access following the matching of precise rules and levels of clearance.

As for the advent of quantum and the security issues it could entail, postquantum cryptography — the design of new protocols based on problems that are also difficult to solve for a quantum computer - **and 'quantum physical security'** — the design of quantum cryptography protocols whose security is based on the laws of quantum physics — **can provide a way to secure cryptography, in fact using quantum to protect against quantum**.

Building resilience means re-assessing processes within organizations, and building a cyber ecosystem including companies, regulators and states.

As threats for corporations are increasingly complex and professionally led, security issues need to be embraced in a **holistic and strategic manner based on people, technology, and the processes**. For people, training and awareness of employees are key as is finding a balance between security and business priorities. Technology is paramount in defense mechanisms with procedures and standards to anticipate 'traditional' malwares and more novel attacks, leveraging innovation such as artificial intelligence. Finally, due process means building plans to react and recover from attacks as quickly as possible.

Beyond the individual organization, calls for building and strengthening 'ecosystem-wide collaboration' and sharing data about cyber-attacks amongst trusted parties are rising. While confidentiality, reputational concerns and uneven levels of cyber maturity have stood in the way of sharing data around attacks has become essential as corporations hold crucial intelligence around the way they are addressing issues, failures, and successes.

Alongside corporate preparedness and collaboration, **regulation has a key role to play in cyber resilience and defense** and regulators are embracing cyber issues, especially since the European General Data Protection Regulation (GDPR) was put in place. Almost everywhere, incentives have become mandatory measures, for example regarding the notification of incidents or data breaches. And **states and international bodies are gradually aligning their thinking to improve global cyber resilience strategies and acknowledging that** cyber space needs to be regulated with global binding frameworks that not only bind nation states, but also the private sector. **Managing cyber risk requires multinational organizations, regulatory bodies, state agencies and corporations to act in synergy**.

Developing cyber insurability depends on the capacity to best model cyber events and to develop the maturity of key stakeholders

Despite the growing issue of cyber risk and the acknowledgement that it is a major area of concern by the public and experts alike, the number of governments and companies that purchase cyber insurance is still relatively low worldwide. As a result, **cyber losses remain mainly uninsured today. However, the demand is growing and accelerating the insurance industry's cyber-cover readiness with the development of appropriate transformations to embrace the challenges of cyber risk coverage**.

Cyber risk is a challenge to the insurance industry in multiple ways — cyber event data is too scarce for recognizing patterns to price the products, cyber accumulation modelling is still at an immature stage and cyber threats are constantly evolving with outsized impact and severe losses. Insuring cyber risks depends on the capacity to model cyber-attacks in a way that integrates the complex dependence effects of cyber events. In response, newer alternative models now capture snowball effects of cyber events as well as their interactions.

To further develop, the industry will have to overcome the limited access to underwriting and risk expertise, including in the innovative realm of autonomous vehicles where data is still based on non-connected models. It will also need to develop the maturity of key stakeholders, such as agents and brokers around cyber risk.

Strategic foresight and sci-fi can help better understand future cyber threats

The uncertainty and complexity around cyber risk illustrates the limits of traditional forecasting and even modelling tools where the future is projected as a logical continuity of the present. Science fiction for strategic foresight can be used to anticipate future cyber threats with ideas that regular frameworks might not otherwise imagine and help prepare for future scenarios and raise awareness.

As threats morph and organizational needs evolve, cyber resilience is, by definition, about being prepared with continual refinement through innovation in modelling, research in threat response strategies, development of new capabilities within the cyber insurance industry and the support of strategic foresight techniques.

Chapter 01

Security and Privacy: Friends or Foe?

Our increasing dependency on technology makes us more vulnerable to cyber threats such as identity theft and email hacks. Solutions to these risks result in techniques that are often invasive and seem to compromise privacy. Are security and privacy opposing goals? Can we balance the dual-use character of cyber technologies? How should we address the societal impact of cyber security measures?

The Double-Edged Sword of Cyber Security

J. Peter Burgess

J. Peter Burgess is professor of philosophy and political science, and Director of the AXA Chair in Geopolitics of Risk at École Normale Supérieure, Paris. His research concerns the meeting place between culture, politics and technology, with emphasis on questions of risk and uncertainty.
He is author of the forthcoming publication **"Terror and Disenchantment: Security after the Unthinkable"**.

> **"Cyber security measures risk advancing societal values in one way, while threatening them in another."**

In January 1961, U.S. President Dwight D. Eisenhower addressed the American public at the end of his term and warned of what would be a central conundrum of the times: the emergence of the 'military-industrial complex'. The simple but powerful notion stems from Eisenhower's observation that the already mastodon armaments industry, a by-product of the privatisation and industrialisation of security, had greater financial interest in war than in peace.

While this specific challenge remains today, its more recent conceptualization is called 'dual-use', which is the ability of any technology to do either good or evil, depending on how it is used. For example, nuclear energy technologies can serve society's energy needs or annihilate populations, rocket engines can launch communication satellites or carry nerve gas and GPSs can guide us to a critically needed hospital or a smart bomb to its target.

70 years after Eisenhower's speech, the prominence of security technologies in society accentuates and intensifies this reality. Indeed, the dual-use issue is particularly salient for security technologies, which hold the potential to do both good or harm. Cyber technologies represent a particularly important example of the conundrum of security and society. The immense societal benefits of cyber technologies coupled with the considerable vulnerability of cyber systems, and the uncommonly high profitability of the cyber industry create a particularly difficult dual-use dilemma.

A good example of the dual-use dilemma in cyber security is the American Colonial Pipeline cyber-attack in May 2021 in the US. The attack was carried out by mobilising cyber technology in order to disable a regional petroleum delivery system managed by cyber technology. When the attack shut down a critical fuel network, the US federal government declared a state of emergency, triggering measures that compromised core US societal values, such as privacy, dignity, trust, care and solidarity.

The central challenge in addressing the societal impact of cyber security measures is the dual-use character of cyber technologies: they both provide benefits to society and present the greatest threats to it. The infrastructure, the expertise, the knowledge and the methods all originate in the same ecosystem. The only defenses we have against cyber risks are cyber technologies themselves.

Since no security guard can fend off a lightning-fast algorithm, cyber surveillance, tracking, profiling, automated analysis and decision-making seem to be the only options. The malevolent activities in cyber space can only be reduced by flooding the entire cyber 'body' with cyber poison and these invasive measures can compromise the exact societal values that cyber technologies are meant to serve, such as privacy, dignity, trust, solidarity, rule of law, civil and human rights, health and safety, among others. A societal approach to cyber security design would first determine which of these societal values cyber technologies generate, and what values are threatened when these cyber technologies come under attack.

Societies in general can be distinguished from one another by the degree to which they regard security as a collective problem or as an individual problem. Whereas Scandinavian countries organise the security of their societies in terms of seeking collective good and avoiding collective bad, highly liberal and individualistic societies like the United States trust that allowing citizens the maximum of freedom to seek the good and avoid the bad will in the end be best for all. Central European countries lie somewhere in between.

The challenge lies in the reality of privatised technology development, as true today as it was for President Eisenhower in 1961. Security in general and cyber security in particular hold the greatest risk in the face of the conundrum that is created when financial values are prioritised over societal values. It is the situation where decisions about what cyber technologies to build and how to build them are based on corporate balance sheets rather than on values and public good.

Privacy and Accountability Need Not Be Opposing Goals

Bryan Ford

Prof. Bryan Ford leads the Decentralized and Distributed Systems Research Laboratory at the Swiss Federal Institute of Technology in Lausanne (EPFL). Since earning his Ph.D. at MIT, Ford has held faculty positions at Yale University and EPFL.
He holds the AXA Chair on Information Security and Privacy at EPFL.

In our digital world, privacy often seems at odds with security and accountability.[1] For example, do we need to know who is behind their screen proposing a service in order to ensure the service is secure and the provider can be held accountable for it – that is, both responsible for complying with rules and able to demonstrate that they are?

> “Giving up our privacy may be insufficient to ensure our cyber security in an AI-led cyber war. Thankfully, it is also unnecessary.”

The early Internet promised a global platform for free expression open to all without censorship or discrimination. However, the massive arrival of anonymous spammers and trolls elicited widespread calls for a stronger identification of users, in order to keep abusers accountable or at least prevent them from creating a new false identity the instant their previous one gets blocked. Now, AI-driven deepfakes can be used to generate millions of false identities and interactions online, amplifying their power of misinformation and chaos by orders of magnitude. These democracy-threatening abuses led to calls for social media platforms to ‘do something’. However, their responses often erode privacy, as anonymous employees and opaque AI-driven algorithms can decide whether each user ‘seems’ human, and their judgements end up unevenly enforced. These algorithms demand massive amounts of privacy-invasive data about users. In addition, the resulting arms race between AI-driven fakery and detection is a war that real humans are doomed to lose.

Now, digital financial platforms such as cryptocurrency exchanges increasingly forbid anonymity outright, cancelling Bitcoin’s early aspirations toward privacy and ‘financial inclusion’, that is, open and democratic financial systems that allow global participation.

Amidst these tensions, it is natural to view privacy and accountability as opposing goals that we must balance. This dichotomy is wrong for two reasons. First, giving up our privacy — even all our privacy — will be insufficient to make user identification truly secure or accountable in the long term if we cannot escape the AI-versus-AI arms race, as cyber wars are in practice often led with AI tools. Second, giving up our privacy may be not only insufficient but also unnecessary. Indeed, typical data-driven approaches conflate identity with personhood, confusing the pool of information about a user with the basic fact of existing as a unique person and the ability to prove that fact securely online.

Approaches driven by Big Data assume that what is important about ‘us’ are bits of identifying information stored in databases: our names, addresses, ID numbers, social media profiles, etc. However, digital information is increasingly forgeable. Relying on information analysis for user identification is both what compromises our privacy and what gets us into the artificial intelligence arms race. India’s Aadhaar program[2] represents a grand experiment in the data-driven approach, aspiring to assign every citizen a unique ID number via biometric identification. Numerous issues of reliability, exclusion, and corruption in Aadhaar, however, have proven a terrifying case study of the risks entailed in assuming that digital information can reliably represent a real person.

Thankfully, collecting and analyzing identifying information is not the only way to achieve accountability online.

As an alternative to privacy-invasive identification — that is, knowing who is doing what online — experimental proof of personhood methods attempt to create anonymous-but-accountable digital tokens that securely and uniquely represent real people without having to identify them.[3] Researchers explore multiple approaches[4] to proof of personhood that exhibit a variety of security and privacy properties.[5] Some of these approaches promise strong security and accountability despite full digital and physical anonymity. For example, digital ‘presence’ tokens can attest that conference attendees are unique and real people without embodying any identity information.

Cryptocurrencies and central bank digital currencies represent another area of tension between security and privacy.[6] Financial compliance regulations require user identification, but this threatens the anonymity, autonomy, and ‘borderlessness’ prized by many cryptocurrency users. Similarly, the perception of central bank digital currencies as tools of digital surveillance by governments and corporations may threaten their adoption. But with technologies for decentralized management of private data, for example, neither cryptocurrencies nor central bank digital currencies necessarily need to accept an ‘either-or’ choice between privacy and accountability.[7] Future digital currencies might be anonymous and even cash-like by default,[8] but could nevertheless enable investigators to follow dirty money trails through warrant-based tracing processes, even without knowing the name or account information of the target.[9]

We must be wary of both the security-purist viewpoint that privacy must be sacrificed on the altar of law and order and the privacy-purist viewpoint that we must live with arbitrarily amplified online abuses as the price of free speech.

The solutions to achieve both security and privacy will lie in the middle. We need better communication and knowledge transfer between the regulators and the technologists who understand and develop these tools.

> “New approaches promise strong security and accountability while preserving full digital and physical anonymity.”

[1] Privacy, Security and Accountability: Ethics, Law and Policy, edited by Adam D. Moore, Rowman & Littlefield Publishers / Rowman & Littlefield International, 2021
[2] Aadhaar Failures: A Tragedy of Errors, Reetika Khera, Economics & Political Weekly, April 2019
[3] Using “Proof of Personhood” To Tackle Social Media Risks, Aengus Collins and Bryan Ford, EPFL, March 2021
[4] Who Watches the Watchmen? A Review of Subjective Approaches for Sybil-resistance in Proof of Personhood Protocols, Divya Siddarth, Sergey Ivliev, Santiago Siri and Paula Berman
[5] Identity and Personhood in Digital Democracy: Evaluating Inclusion, Equality, Security, and Privacy in Pseudonym Parties and Other Proofs of Personhood, Bryan Ford, November 2020
[6] Design Choices for Central Bank Digital Currency, Sarah Allen et al. Global Economy & Development Working Paper 140, Brookings Institution, July 23, 2020
[7] CALYPSO: Private Data Management for Decentralized Ledgers, Eleftherios Kokoris-Kogias et al., August 2021
[8] How to Issue a Central Bank Digital Currency, David Chaum, Christian Grothoff and Thomas Moser, Swiss National Bank, March 2021
[9] Open, Privacy-Preserving Protocols for Lawful Surveillance, Aaron Segal, Joan Feigenbaum and Bryan Ford, July 2016

Chapter 02

Mitigating Cyber Risk – from Critical Infrastructures to Quantum

The future of cyber security is shaped by the ever-changing nature of cyber space coupled with the computing speed of today's machinery, and the acceleration of artificial intelligence and machine learning capabilities. This provides increased opportunities for malevolent attacks. In this environment, are we able to retrofit resilience into existing critical infrastructures built with traditional risk-based approaches? How can we tackle the security challenges linked to cloud-based operations? Can we prevent our machine learning algorithms from being fooled by another artificial intelligence? Will our information still be secure once the quantum computational power becomes strong enough to decrypt every protection we set?

Designing and Retrofitting Resilience into Critical Infrastructures

Giovianni Sansavini

Giovanni Sansavini is an Associate Professor of Reliability and Risk Engineering at the Institute of Energy and Process Engineering, ETH Zurich. He holds the AXA Chair at the ETH Risk Center and of the Technical Committee on Critical Infrastructures of the European Safety and Reliability Association. Giovanni Sansavini received his B.S. in Energy Engineering and M.S. in Nuclear Engineering from Politecnico di Milano, in 2003 and 2005. In 2010, he received his Ph.D. in Mechanical Engineering from Virginia Tech and in Nuclear Engineering from Politecnico di Milano.

> “Many infrastructures are critical to the workings of our societies. They can be designed or retrofitted to promote cyber resilience.”

In order to maintain societal welfare, ‘critical’ systems and sectors are indispensable. Most of these sectors or industries are essential for the continued workings of our societies by providing services such as heating and clean water to meet the basic life needs, as well as electricity supply for manufacturers and the financial sector.

Cyber-attacks on any of these sectors or a piece of infrastructure can cause mayhem, as illustrated by the 2021 ransomware attack on the Colonial Pipeline, which has prompted gasoline shortages and panic buying in the southeastern United States.[1] Whether a piece of infrastructure is considered critical reflects our societal standards and values. Some sectors are deemed critical in one country but not in another, such as commercial facilities or the defense sector. In practice though, there are a lot of similarities.

The current approaches to protecting critical infrastructures from cyber risks are similar to those developed for non-critical infrastructures. They include very well-established risk assessment and risk management processes defined in international standards, such as the ISO (International Organization for Standardization) standards, and ensure that there are no major issues in the nuclear sector or in space missions for instance.

However, there are limitations to such a risk-based approach. With cyber risks in particular, there is a lot of uncertainty around the nature and magnitude of the threats and on their evolutions. In addition, for some risks, we simply do not know the consequences of a hazard, for example those of a specific chemical spill on human health or on the environment. This type of hazard in the physical world can be related to cyber threats in ways we don’t always see at first. Consider the near miss cyber-attack on an American water treatment plant in 2021,[2] where hackers tempered the level of sodium hydroxide by a factor 100, which would have made the water dangerous to drink. In that case, the tempering was stopped by human intervention before the water quality was affected, but there were additional safety mechanisms, such as sensors, that could have helped as well. We call these ‘additional layers of protection’.

The idea of ‘layers of protection’ is part of the novel approaches that focus on resilient designs. Indeed, we now design systems so that they can sustain some level of impact and destruction because we acknowledge that we ignore some of the threats and hazards. In some sense, we need to be agnostic to the type of threat we are facing to complement the risk approach.

Modern society relies on networks. We are interconnected in everything from food supply and water treatment to energy supply. Networks allow us to balance commodities and be more efficient. The electricity network for instance is used to balance excess electricity produced in one place to another place with less supply at that time. However, networks also make us interdependent. In 2015, Ukraine suffered from a cyber-attack on its power grid, cutting the electricity supply of 225,000 people.[3] As the European electrical network is interconnected, instabilities could also have cascaded to a rather large scale. Luckily, we have standards for such technical and international networks that national operators comply with diligently. To ensure the commodity remains available when there is an issue at one point of the network, such as a blackout in an interconnected country, an option is to have ‘buffers’ like local suppliers in place. For other types of networks however, we do observe dramatic cascade effects. The July 2021 ransomware attack on Kaseya, an American IT Management Software provider, led to tens of thousands of computers locked up across the globe, and the hackers demanded $70 million to unlock all the affected systems.[4]

Sometimes, partners temporarily no longer wish to be connected. This happens when part of a system is infected, as with the cancellation of international flights during the Covid-19 crisis. A resilient design ensures that the system is able to work in ‘islanding mode’ with islands working independently. Another design adaptation is to have flexibility in the modes of operation, for instance using complementary supplies such as oil and electricity supplies in case the electricity network, or a pipeline, goes down.

These design adaptations are doable on existing infrastructures by retrofitting in their designs or adding layers of protection. This comes at a cost, but we do need to exploit infrastructures that already exist at best, as building new infrastructures has important impacts, not least environmental ones. However, some infrastructures simply do not exist yet, for example, carbon dioxide storage and distribution networks, and hydrogen production and distribution networks. Designing these networks from scratch means we can use the principles described above — islanding, buffers, flexible operation — and others to make our connected infrastructures resilient by design.

[1] DHS to Issue First Cyber Security Regulations for Pipelines After Colonial Hack, Ellen Nakashima and Lori Aratani, The Washington Post, May 25, 2021
[2] ‘Dangerous Stuff’: Hackers Tried to Poison Water Supply of Florida Town, Frances Robles and Nicole Perlroth, The New York Times, February 8, 2021
[3] Hackers Behind Ukraine Power Cuts, Says US Report, BBC, February 26, 2016
[4] Ransomware Hackers Demand $70 Million to Unlock Computers in Widespread Attack, Robert McMillan, The Wall Street Journal, July 5, 2021

New Strategies to Enhance Cyber Security in the Cloud

Robert Deng

Robert Deng is AXA Chair Professor of Cyber Security, Director of the Secure Mobile Centre, and Deputy Dean for Faculty & Research at the School of Computing and Information Systems of Singapore Management University. He is a Fellow of IEEE and Fellow of Academy of Engineering Singapore.

In about two decades, cloud computing has seduced virtually all organizations of all sizes on Earth as it brings many benefits such as rapid deployment, low up-front costs and scalability. Indeed, instead of owning their infrastructures for their software, hardware and data storage and having to maintain them, organizations have by and large turned to cloud-based operations, where they share infrastructures and sometimes services with other users.

> “In security, the biggest enemy is complexity.”

This change towards shared infrastructures means new security challenges, including massive data breaches and hacks into computing resources to mine cryptocurrencies. Why is that?

Indeed, security challenges arise as cloud computing is less secure than on-premise computing. In traditional on-premise information systems, the physical infrastructure, the hardware and the software are all located within the organization. The organization can control everything and has a good visibility of what is happening in its own information systems.

Because of the virtualization of machines, servers, etc. in the cloud, you have different components at different locations, provided by different service providers. This means that the environment is very heterogeneous. Neither the data owner, nor the consumers, nor the service providers have full control over the whole environment. They even have little visibility over the system, which means that a breach may occur without anyone noticing.

In addition, in the cloud, what we call the ‘attack surface’ is much larger than in on-premise information systems: the system has more vulnerabilities and more exposure to cyber-attacks. Vulnerabilities can be in the machines themselves, on the service provider side, and also on the user side, for example, in a phishing attack, where users disclose their credentials.

What is the ‘Zero Trust’ strategy that now leads cloud security efforts worldwide?

So far, we have always assumed that we could trust our servers and operating systems to keep our data confidential, to authenticate the user correctly, to enforce access control. This worked well for traditional on-premise computing. Today, in the cloud, it is a much riskier assumption, but unfortunately still made by many.

The Zero Trust strategy is to not automatically trust infrastructures, devices and service providers. Rather, we think trust needs to be established based on different principles. An example is to create secure spaces separated by gatekeepers. For example, you might want to setup a firewall between an application server and a database server that contains confidential data.

Another principle is multi-level security control. If one layer of protection breaks down, a second layer is still up and running, protecting our information assets. For example, if the login access into your user account in cloud storage is breached because an attacker found your password, data encryption acts as a second layer of protection. Two-factor authentication relies on this principle.

A third principle is to follow the best security practices, for example follow the ’least privilege’ principle, which would be the numerical equivalent of granting access on a ‘need-to-know’ basis.

In the cloud, controlling access at every entry point soon becomes overwhelming. What are the strategies to tackle the scalability challenges related to distributed environments?

Models for access control that were designed for centralized information systems can work well for many distributed information systems.

The first option is ‘discretionary access control’: the data owner decides which user can read their data, or edit it, or own it. Even with a very distributed system, discretionary access control works well. Another option is ‘mandatory access control’, which is used in governments and the military for classified information. The data is labelled, depending on its required security levels. Each user is given a security clearance. If the label and the clearance match, access is granted. Finally, a variation is to have ‘role-based clearances’. This is useful when you have a rapid workforce turnover for example. Instead of giving access privileges to the user directly, you give privileges to a role, and whoever is holding that role will get the relevant clearance for their positions.

The Internet-of-Things (IoT) is an extreme example of a distributed environment. Are IoT security challenges different from cloud security challenges?

In cloud computing, the data center is managing the data and providing services, there is still some centralized management. The Internet-of-Things is a huge, complex and open environment, with a variety of users and devices, including physical objects with little computing capability and little battery-life: door locks, lights, etc. They cannot afford to be encrypted with strong security measures or solutions, and a common example of attack is the ‘Distributed Denial-of-Service’, in which an attacker sends so many requests that devices are overwhelmed and hang. In other words, the system complexity of the Internet-of-Things can grow beyond anyone’s ability to manage it.

> “Finding a good technical solution for access control in Internet-of-Things is an open research question today.”

Finding a good technical solution for access control in Internet-of-Things is an open research question today. I believe that IoT security requires a different approach: more security regulations and more public security awareness education to the common users. This could be done for example using certification: products such as CCTV cameras could be certified for specified security levels, to encourage users’ awareness and manufacturers to produce more secure devices.

AI and Machine Learning: Defense Mechanisms That Need to Be Defended

David Rios Insua

David Rios Insua is AXA Chair in Adversarial Risk Analysis at ICMAT-CSIC and Member of the Spanish Royal Academy of Sciences. He holds the DeGroot Award from ISBA and led the Games and Decisions in Risk and Reliability program at SAMSI. He has held research and/or teaching positions at Duke, Purdue, IIASA, Aalto, Paris-Dauphine, Shanghai University for Science and Technology, CNR-IMATI, UCM, UPM and URJC.
He is a specialist in Bayesian analysis, decision analysis and risk analysis and their applications to security and cyber security. He is Scientific Director of Aisoy Robotics.

> “We use modern machine learning and AI tools to design more cyber secure systems, but we need to design machine learning and AI so that they are unaffected by attacks.”

Machines are getting increasingly smarter. Cars can now help you plan your itinerary and help you park, sensing the trees, pavements and surrounding vehicles and activating the brakes as needed. In a not-so-distant future, they might routinely transport us from home to work in a driverless manner. They gather and transmit data and learn on the go, powered by artificial intelligence in a globally connected world. Are smart connected machines going to make our world more secure or, to the contrary, less so?

AI is now used by cyber security companies and governments to track down unknown vulnerabilities in their information systems and fix them before attackers exploit them. For example, automated systems can check the status of hundreds of thousands of connected devices and send warning signals to engineers when a device behaves abnormally, signalling a potential intrusion. Predictive models can also forecast imminent failures, and AI then offers precious time to react in advance.

In addition to mere scanning systems, some threat intelligence systems perform in-depth analysis of the security environment and posture within an organization. However, the entailed data deluge needs to be coherently aggregated to provide meaningful and useful risk indicators, and a combination of machine learning and economic models aid in performing such an aggregation. Threat intelligence systems can also analyze web and social network content, looking for negative online mentions of a company, which constitute a reputational threat but could also trigger cyber-attacks. This goes further than scanning, as ascertaining the nature of the tweets for example relies on advanced AI tools, such as language and sentiment analysis.

In all these cases, AI supports cyber security decision making in the presence of adversaries. New approaches, such as adversarial risk analysis, facilitate online decisions and enhance accuracy and speed in cyber risk management.

However, while the list of AI applications requiring strict security is endless (automated driving, content filters, policing and so on), AI is not immune to cyber-attacks itself. To ensure that AI applications are secure, machine learning algorithms need to be robust and reliable.

Indeed, while state-of-the-art machine learning algorithms perform extraordinarily well on standard data, they are vulnerable to so-called ‘adversarial attacks’. These attacks use data crafted precisely to fool AI. The first instance of this type of attack targeted a machine trained to recognize panda pictures. The attack led the machine to recognize a panda with high confidence when the picture was in reality, replaced by a picture of a gibbon. To achieve this, attackers simply needed to interfere during the machine learning process, presenting data that is falsely labelled — here, passing gibbons for pandas during the machine training phase. In real life, a worrying equivalent is that an autonomous car can be fooled into reading a stop sign as speed limit, and therefore not stop at the sign. Fraudsters could also disguise illegitimate insurance claims, fooling the corresponding algorithm to receive compensation. Quite importantly, attackers quickly adapt to the defense machine learning systems in place, and this could have dramatic implications in domains such as automated driving systems, defense systems, law enforcement and health to name a few.

These security issues question our standard algorithm design methods, given the presence of adaptive adversaries ready to intervene in the problem to modify the data on which we rely.

To avoid adversarial attacks, a new field called ‘adversarial machine learning’ is emerging. Its aim is to make machine learning systems robust against malicious attacks. This entails studying attacks but also defenses against attacks. For example, in spam detection, we have deployed classifying systems to detect and stop spam, but then attackers learned how to fool the protection system by changing critical words (instead of Viagra, they use VE@ GR@) to make the antispam system think that a message is legitimate. We have had to learn about evolving attacks, in order to incorporate better defenses without stopping legitimate mail. The ‘adversarial machine learning’ research field uses mostly game theory to model the confrontation between learning-based systems and their adversaries.

However, in ‘adversarial machine learning’, we often assume that defenders and attackers share some information and knowledge. This assumption about sharing common knowledge is questionable in the security domain, as adversaries of course try to conceal information from each other. So we are developing another way to handle adversarial machine learning, called ‘adversarial risk analysis’, using forecasting. We model how attackers attack and react, and use this knowledge to forecast how they might attack in the future, without using the strong assumptions regarding a shared, common knowledge.

Cyber security and AI go hand in hand. As with many tools and methodologies, AI is a double-edged sword: we use modern machine learning and AI tools to design more cyber secure systems, but we need to design machine learning and AI so that they are unaffected by attacks. We need cyber security to become even more intelligent.

Quantum: An Additional Threat?

Antonio Acín

Antonio Acín is an ICREA Research Professor at ICFO-The Institute of Photonic Sciences. He has a degree in Physics from the Universitat de Barcelona (UB) and in Telecommunication Engineering from the Universitat Politècnica de Catalunya. He got his PhD in Theoretical Physics in 2001 from the UB. After a post-doctoral stay in Geneva, he joined ICFO in 2003. At ICFO, Prof. Acín leads the Quantum Information Theory group. He is also AXA Chair in Quantum Information Science since 2016.

> **“Quantum algorithms and computers will impact cyber security, but we can already prepare our systems for quantum resilience.”**

In ancient Rome, if you wanted to share a secret message with an ally far away, you would have used the Caesar code, one of the most famous and simplest encryption techniques. Letters in the message were shifted some fixed number of positions in the alphabet: for instance, A becomes I, B turns into J, and so on. Today, we all use cryptography on a daily basis, for instance through debit card payments, email exchanges or critical data transmission. Cryptography is essential for our cyber security and encryption techniques have of course dramatically evolved.

Cryptography is the art of sending private information in a secure way. Nowadays, it is mostly based on computational security: existing protocols are secure because hackers need to solve a problem for which no efficient algorithm is known. For example, to connect to your favourite websites or for remote connections, you daily use the RSA protocol, which is based on the fact that there is no efficient algorithm to factorize large numbers. Computational security is convenient because it is cheap: it is a software solution and does not require buying any device, just running a program. However, computational security is also risky.

Indeed, the advent of quantum computers, which exploit the collective properties of quantum states such as superposition and entanglement,[1] sheds some doubts on the applicability of some security algorithms, because quantum phenomena will give quantum computers a very large computational power. In 1994 already, the famous Peter Shor, at Bell Labs at the time, designed an efficient quantum algorithm for factorization. An eavesdropper with a quantum computer will be able to factorize large numbers and hack RSA. This is not currently perceived as a risk, because as far as we know nobody has the technology to create a quantum computer powerful enough to run Shor’s algorithm at the moment. However, are we sure about this? And even if this is indeed the case, how long will it take for someone to have such a powerful quantum computer?

But even without a quantum computer, there is no proof that no classical efficient algorithm exists to solve the problems exploited by cryptographic protocols. In the case of RSA, it is in principle possible that a non-quantum algorithm for efficient factorization already exists. It seems unlikely simply because so many attempts to find such an algorithm have failed so far. But one cannot exclude that someday, smart hackers will find efficient non-quantum algorithms that turn our security into a mere illusion.

To alleviate these risks, two approaches are possible. The first one is to maintain the paradigm of computational security and to design new protocols based on problems that are also difficult to solve for a quantum computer. This is known as ‘post-quantum cryptography’ and has a big advantage: it is again a software solution, hence cheap, and its integration with existing infrastructures is straightforward, as you only need to run a different program. It maintains, however, some of the previous risks: there is and will be no proof of the non-existence of an efficient algorithm. We cannot exclude the possibility that a smart hacker equipped with an efficient algorithm breaks the protocol.

The second approach is ‘quantum physical security’, a change of paradigm in security applications. Using quantum phenomena, it is possible to design quantum cryptography protocols whose security is based on the laws of quantum physics. An eavesdropper aiming at hacking them would not need to solve a complex computational problem, but to hack the quantum implementation. The big advantage of quantum cryptography protocols is that security can be proven. The main disadvantage is that it is a hardware solution: you need to buy a separate and expensive device. Because of that, the security may be sensitive to the implementation, and the integration with existing infrastructures is harder.

The best approach going forward is to combine both quantum physical security and quantum-resistant cryptography. On the one hand, by designing post-quantum protocols with as much evidence as possible of their resistance against quantum computers. On the other hand, by developing cheaper quantum cryptography protocols and improving their integration in existing infrastructures, so that a layer of quantum physical security can be added to strengthen our encryption techniques as soon as it is technically possible. Secure communication is a tentacular issue, where various levels of confidentiality, risk and budget, amongst others, need to be considered. Having more tools to face all these challenges only makes us stronger and it is now clear that quantum physics provides new recipes to ensure our secrets remain secure. With the two approaches combined, hackers will have a much more difficult time, as they will have to face complex computational problems and quantum phenomena at the same time.

[1] How Does a Quantum Computer Work? Michael Tabb, Andrea Gawrylewski and Jeffery DelViscio, Scientific American, July 7, 2021

Chapter 03

Cyber Resilience of Organizations and States

Building cyber resilience entails action from all economic players — the private sector, states and international bodies. What does that mean for private organizations? How can the private sector partner to be collectively more resilient? How is cyber space being regulated, if at all? What are the success factors to move forward collectively in the arena of cyber security? What is the role and stance of states?

Building Cyber-Resilient Organizations

Arnaud Tanguy

Arnaud Tanguy is AXA Group Chief Security Officer. He leads information security, physical security, health&safety and operational resilience of the Group. He previously was the Chief Information Security Officer (CISO) at AXA Investment Managers in charge of the global information security program across all lines of business.
Prior to joining AXA, Arnaud was a Senior Manager at PwC and EY specialized in information security and IT strategy. He began his career as an officer in the French Navy leading the department in charge of IT, telecommunications, and information security at the naval base of Brest.

With software vulnerabilities, insider threats and employees disregarding security measures, organizations face cyber risks related both to their own personnel and to outside threats.

> “Security-by-design is how we now need to conceive every project in the company.”

What does cyber resilience mean for organizations?

Cyber resilience requires anticipation and a systematic and rigorous approach to be ready to face the unknown. Being resilient not only means avoiding incidents, but also being ready to recover from the worst-case scenario. Cyber resilience is definitively a challenge in a cyber space where things are moving so fast. All organizations in the future must be capable to serve their customers, employees, and investors regardless of the cyber challenges they may face.

What are the concrete implications of a cyber-attack for a company, a data theft for example?

A data breach occurs when individuals get access to data that they then can leak, sell and use for identity theft, so the first risk is really to the people that the data belongs. The second risk is for the company, as it can fail to comply with regulations that now typically include mandatory notification of individuals whose data has been compromised for example. Reputation is another issue: while the company is the victim, its name is the one that appears in the media and this can lead to issues with customers’ trust and missed opportunities. The legal risk relates to the fact that many contracts do not yet include security clauses that describe the security measures that have to be put in place by the client, creating legal loopholes. Finally, the financial impacts of an attack are numerous, as quickly remediating the vulnerabilities, communicating with the media and customers, possibly millions of them, compensating customers and sometimes even paying fines, can all generate important costs.

What measures do private organizations take to limit cyber risks?

Threats are increasingly complex and professionally led, so security issues need to be embraced in a holistic and strategic manner. It starts with people, whose awareness and preparedness can be raised through internal communications, mandatory training or even fake phishing campaigns. We train our employees as cyber citizens and hope they will discuss it with their friends and families, so that we participate in training society at large, through our own people.

Finding a balance between security and business priorities can remain a challenge but there is now a good awareness in executive boards. It helps taking the right decisions on security measures while supporting the business means.

Security teams must find the right security level from the inception of each project, a principle we call ‘security-by-design’. In addition, any third part of a company could be subject to an attack, and security clauses are needed in provider agreements. The tech side implements technical measures, procedures and standards to anticipate ‘traditional’ malwares and more novel attacks, leveraging innovation such as artificial intelligence, and monitors activity to ensure our security measures are adequate. Finally, we build plans to react and recover from attacks as quickly as possible.

The same principles apply everywhere. Whether or not there is a dedicated internal team in the company, there must always be someone responsible and accountable.

How are regulators helping to guide corporations towards more security?

Regulators are embracing cyber issues, especially since the European General Data Protection Regulation (known as ‘GDPR’) was put in place. Almost everywhere, we went from incentives to mandatory measures, for example regarding the notification of incidents or data breaches.

For a company, it is advantageous to engage early with regulators, to be transparent and build trust, as it helps in solving issues faster. Of course, this can be a challenge for multinationals: AXA for example works with 64 different countries and we engage with 64 regulators that each work differently.

> “For a company, it is really advantageous to engage early with regulators, to be transparent and build trust, as it helps in solving issues faster.”

Some companies specialize in providing cyber security services to their clients, for example organizing audits and providing security tools. What is their role in building a more cyber resilient world?

For a private company whose main business is not related to cyber, for example a supply chain company, collaboration with cyber security providers is key. Indeed, there is a real arms race, with the speed and scope of attacks growing rapidly but we haven’t, as a society, trained enough people in the cyber domain and the cyber security workforce market is very competitive. Companies that provide cyber security services are able to pool these talents, to bring advanced capacities in cyber defense, such as automation. In short, cyber security service providers help organize the ecosystem efficiently.

Providers bring knowledge of the attacks, data collection and threat intelligence as well as innovations in the services they provide, while internal teams know their business in depth, the sector, and the history of the company. These internal teams are also hybrid ones, as they are composed of IT experts and of business people who make the link between the assets that need to be protected and the protection measures that the company uses. Working in partnership across the board is a necessity.

Cyber Resilience in the Post-Pandemic World – An Urgent Need for Data-Sharing and Co-Operation

Heyrick Bond Gunning

Heyrick Bond Gunning is the CEO of S-RM, a global intelligence and cyber consultancy. Before S-RM, he was a Managing Director at Kroll – prior to which he consulted for DHL in Iraq in 2003 and 2004, following the end of the Iraq War. From 2000 to 2003, Heyrick was the Head of Client Engagement for Mergermarket (Acuris). He started his career with 5 years in the British Army. Heyrick has a BA in Geography and Archaeology from the University of Manchester and is an INSEAD alumnus.

Since the beginning of the Covid-19 crisis, phishing attacks have targeted remote-workers, ransomware attacks on hospitals have increased, and a stock exchange was even closed by an old-style distributed denial-of-service attack.

Beyond the number of cyber-attacks that seems to have increased in frequency and in scale, have the type of attacks also changed?

With Covid-19, between March 2020 and March 2021, the number of ransomware attacks we had to deal with was multiplied by 4. They now represent about 50% of the ways data is being breached, and it is a dynamic, evolving threat. Traditionally someone would encrypt your data and demand a ransom to decrypt it. Today, they'll take the data, encrypt it, and because they understand the reputational risk and regulatory risks, they'll threaten to start talking about the attack publicly. They now use two levers and it's called 'double extortion'.

Has the pandemic shifted cyber security priorities?

At a very practical level, one challenge comes from using personal devices for work, such as phones and computers. Policies and procedures around this have always been important, but they are going to be at the forefront of cyber resilience going forward, as many parts of the world are going to continue to embrace flexible remote working practices. With this hybrid model of working, there are very difficult questions about how to balance the privacy of the employees with ensuring that the correct protections are in place for the work data.

Another shifting priority for the future is the question of how cyber risks will be insured. The insurance sector is talking a lot more about what services can be used to reduce the risks, including advice and training to the clients, such as in-depth reports on their threat picture, establishing plans to activate in case of a breach. The first 72 hours can more than double the cost of a recovery, if the situation is handled badly at first.

Does the way we assess risk and organizational cyber resilience need to evolve?

Even before Covid-19, there were questions around the usefulness and value of 'cyber readiness metrics', and the pandemic has introduced even greater uncertainty. It has led to a further reduction of the confidence of security teams and corporate leaders about their ability to understand and tackle the most important cyber issues.

However, the three key points to consider remain the same: the people, the technology and the processes. One needs to ensure that everyone is trained and knows what to do in case something suspicious occurs. Then, while technology is useful, it can be relied too heavily upon, especially when people don't understand it. People and technologies go hand-in-hand, what binds them are the processes. In particular, having a plan for when it all goes wrong. One needs to think about the worst-case scenario prior to something going wrong, because it will be really difficult to think clearly in the midst of a ransomware attack.

We ask four key questions to assess cyber readiness: Do you know who your adversaries are? Are you focusing on the right risk? Does your response plan reflect the most likely threat scenarios and have you tested it? Do you have a roadmap to recover in the event of an incident, or in other words: how are you going to get your systems back and running?

That's even more important now, as data compromise within a business has become very likely -- it may take the form of an attack, a mistake an employee makes or an action an employee takes because they're disgruntled for example.

What are the challenges to putting in place a more resilient ecosystem?

First, the big challenge is obviously the scarcity of data. The cyber sector is new and cyber threats are very dynamic and difficult to model. The best strategy in that case is to map out the decision that one would like to make, identify the information that one needs to make these decisions and make a plan about how you will collect that information.

Indeed, the lack of data also comes from a lack of sharing the information. Companies actually hold intelligence -- the way they are addressing issues, their failures and successes. But people are reticent around sharing their intelligence, even within a company. Externally, companies avoid sharing the information due to reputational concerns and regulatory concerns, as some attacks may let a company fall foul of some regulatory constraints.

To build an ecosystem, it comes down to building relationships and trust. I see different areas that can be worked on, for example when same-level experts from different IT departments are able to discuss best practices freely. Companies could agree on an external information-sharing scheme for certain elements of the data. Finally, an important point would be to communicate regularly with the regulators, who usually become more open once a relationship is built.

Are states and international bodies aligning their thinking to improve global cyber resilience strategies in a post-Covid-19 world?

One of the big challenges with cyber is that it has no boundaries, it's a global issue. In many ways, it takes the same form as a pandemic and requires multinational organizations, regulatory bodies and state agencies to act together.

A big turning point for businesses to start really thinking about cyber and data protection was actually GDPR — it was rolled out in 2016 and a good example of international regulation having real impacts.

International alignment is very difficult because everyone has vested interests, but where there seems to be some form of coalescing of agreement now is around the payment of ransoms to terrorist organizations, as opposed to criminal organizations, and around the relation between terrorism financing and cyber security. I think that's where we'll see the biggest change in the coming years. For example, the Office of Foreign Assets Control in the US has a list of people that need to be checked against to prevent terrorist financing — in other words, companies need to be extremely cautious when they pay a ransom, to ensure the organization is 'just' criminal and not terrorist. It's really challenging to know, but there are a few hidden clues sometimes, such as the bitcoin wallet used, or the way communications are held with the victim.

> “Are you focusing on the right risk? Does your response plan reflect the most likely threat scenarios and have you tested it? Do you have a roadmap to recover in the event of an incident, or in other words: how are you going to get your systems back and running?”

Cyber Ecosystems against Cyber-Crime

Nicolas Arpagian

Nicolas Arpagian is Cybersecurity Strategy Director of Trend Micro. He is also Advisor to Mr Michel Van Den Berghe, appointed by the French Prime Minister to build the Cyber Campus, a hub of cyber security that will bring together the main national and international actors in the field to federate the cyber security community and develop synergies.

> “While it may seem counterintuitive to discuss weaknesses, sharing data around cyber-attacks has become absolutely essential.”

The cyber ecosystem is extremely large. In the digital world, physical barriers are removed and anyone with an internet connection can partake in cyber activities, legal or fraudulent. A portion of the population uses illegal ways to watch live video streams of soccer matches for example, without really defining themselves as hackers.

International organizations have started talking about ‘cyber ecosystems’ against the cyber-crime industry. The World Economic Forum, amongst others, provides guidelines to improve cyber resilience, including strengthening ‘ecosystem-wide collaboration’ and sharing data about cyber-attacks amongst trusted parties in the same economic sector or economic chain. This type of recommendation has existed but confidentiality, reputational concerns and uneven levels of cyber maturity stood in the way of sharing information on attacks: discussing weaknesses is not something that companies traditionally like to do, especially as these new partners in the cyber security ecosystem might be competitors on the business side, for example clients or providers. However, sharing data around attacks has become absolutely essential.

To partake in such an ecosystem, corporations must consider two things. First, cyber risks cannot be avoided: it is not a question of whether an attack is going to take place but rather when will it happen. Second, there will always be a ‘patient zero’, the first entity to be infected. Partners need to go beyond the stigma of being the victim of a cyber-attack. Creating an ecosystem where trusted partners share data about cyber-attacks allows for a better understanding of the point of view of attackers. A member may realize that a business software they use has a vulnerability or that this vulnerability has been compromised, and know that many other companies in the same business sector use the same software and are therefore at risk or already under attack.

In practice, there are several important ingredients in building a resilient ecosystem. Ahead of the attack, partners need to know and trust each other, to have agreed on their strategy and confidential communication channels. They also need to know how to document the attack in a way that is useful to others. To do so, imagining that someone else is the victim and is giving you the intelligence you need helps: you would want to know the context, what happened, what the symptoms were and how the attack was handled.

An ecosystem goes much beyond economic interests. It requires seeing the world in a transverse fashion, as some of our cyber tools are shared across sectors. It’s a very new way to do things.

While states cannot mandate ecosystem-building to fight cyber-crimes, they can incentivize it. They can explain why this would be advantageous, they can highlight the practices that have proven their worth in various sectors, for example organizing circles of trust where the companies can share information about current cyber threats or helping universities or IT programs to have professional training sessions to guarantee that all students have the opportunity to learn about the main legal and technical aspects of cyber security.

The cyber ecosystem includes companies, regulators and states, all composed of humans of talent. Cyber security is recruiting. Civil administrations, armies, medium and large companies, service providers, and criminal organizations all need experts. In many developed countries, there is a shortage of candidates, because existing training programs do not recruit enough. I believe that co-optation might be a solution, as it emphasizes shared values and in particular ethical values. Another option for the larger companies is to transfer people with technical expertise and loyalty into cyber security departments within companies. We also need to showcase how varied the jobs are in cyber security, from crisis management to training, audit and consulting, and technical developments for example.

Organizing and Regulating Cyber Space

Guillaume Poupard

Dr. Guillaume Poupard is the Director General of the National Cyber Security Agency of France (ANSSI) since March 2014. He graduated from École Polytechnique then obtained his PhD in cryptography from École Normale Supérieure in 2000. He became Head of the Cryptography Laboratory at the Central Network and Information Security Directorate which formed in 2009 the basis of ANSSI. He joined the Ministry of Defense in 2006 and was appointed Head of the Cyber Security Division within the Technical Branch of the National Defense Procurement Agency (DGA) in 2009. (©Patrick Gaillardin)

Juhan Lepassaar

Juhan Lepassaar is the Executive Director of the European Union Agency for Cyber Security (ENISA) since October 2019. Prior to joining ENISA, he worked for six years in the European Commission, including as Head of Cabinet of Vice-President Andrus Ansip responsible for the Digital Single Market. In this capacity, he also led and coordinated the preparations and negotiations of the Cyber Security Act. Juhan Lepassaar started his career in EU affairs with the Estonian Government Office, leading for five years the national EU coordination system as the Director for EU affairs and EU adviser to the Prime Minister.

> “Regulations can be part of the solution, if done correctly.”
>
> G. Poupard

From espionage to ransomware to critical infrastructure interference, cyber threats disrupt the welfare of individuals and companies and the security of states and democracies. We have one foot in the physical world and the other in a digital, immaterial space, where a large part of the battle for influence and money takes place.

How does cyber warfare compare to previous types of wars? Is it building a new balance of power?

Guillaume Poupard: The term “war” is adequate for cyber conflicts but different from what we knew in the past. In cyber-crime, there are a variety of attacks, attackers and victims. Some states aim to spy on each other, while some others want to start actual wars, albeit in the digital space. Leading a cyber war nowadays is relatively cheap, as a cyber army can amount to just a few hundred people. However, powers such as the US, Russia or China, invest massively on both offensive and defensive cyber arsenals, and one of their first goals is to make sure that they remain the strongest forces in this domain. Both new types of attacks and renewed strategies from the past are within the immense range of possibilities offered by cyber-attacks.

Juhan Lepassaar: In the case of cyber warfare, if several players — including sovereign nations, corporations and individuals — don’t take steps to change their behavior, the number of cyber-attacks will increase indefinitely. New vulnerabilities and their impacts appear frequently in climate change issues. It is similar in cyber as we haven’t yet fully realized the impacts of all the vulnerabilities that can be exploited. The behavior of people, processes, legal systems and political frameworks that we build around cyber matter a lot. Everyone can do something that may seem tiny but absolutely necessary about this global problem.

How can we build a global framework to avoid cyber wars?

GP: The mechanisms we use to control traditional wars do not apply to cyber. For example, as a computer program can simply be sent by email for legitimate purposes as well as warfare, our previous arrangements to limit arm exportations become irrelevant in this case.

International efforts are underway to account for this new situation. For example, the United Nations Group of Governmental Experts and the Open-Ended Working Group discuss laws and regulations for cyber space. States disagree on many things but agree that discussion on cyber is necessary and that this new space cannot remain without rules. The issue is therefore, as often, to confront different cultures and political approaches. In France, for example, we talk about the ‘security of information systems’, and never use the terms ‘security of information’ because, to us, that leans too closely towards the ‘control of information’: we prefer to focus on the infrastructure rather than on

> “The machinery used to power the cyber realm is often owned by the private sector and isn’t controlled by states, so we need to look at global binding frameworks that not only bind nation states, but also the private sector.”
>
> J. Lepassaar

> Cyber security is everybody's problem. From individuals to states, industrial alliances and consumer groups, we need to raise awareness and set up regulations.
>
> G. Poupard

the content. However, other countries make direct links between the security of information systems, the security of information and the control of information. This has been a major limit on international discussions so far.

JL: The machinery used to power the cyber realm is often owned by the private sector and isn't controlled by states, so we need to look at global binding frameworks that not only bind nation states, but also the private sector. However, the states and alliances like the EU are responsible for ensuring that the regulatory frameworks they design are applicable in real life.

It is important to understand that cyber space is not operated and controlled by a small and well-defined number of players but by an immense multitude: we need to look at these actors holistically. We also need a better understanding of the 'duty of care' in cyber space: what are the responsibilities of each actor within the cyber space?

What is Europe's approach towards a more cyber secure world?

JL: We have a prudent risk-based approach in trying to build up a more resilient cyber space. So far, our work has focused on critical sectors looking at the minimum requirements that everybody should follow. However, as we observe with global warming, that might not be enough. So, we start thinking about cyber products and services, about sharing information within Europe, and about setting up common standards for all the cyber actors: what is expected, how to reassure society. Another important area is the security of our supplies: in some areas, we should have stronger digital autonomy, stronger industrial and research capabilities and better investment, to ensure that we can build a resilient environment.

GP: Cyber security is everybody's problem. From individuals to states, industrial alliances and consumer groups, we need to raise awareness and set up regulations. Regulations can be part of the solution, if done correctly.

In practice, how do states and alliances organize their cyber offense and defense capabilities?

JL: The main goal of the European Union Agency for Cyber Security (ENISA) is to ensure that the internal market remains functional and is not affected by cyber-attacks. This goes through capacity building for example, so that actors are mature enough to respond, or through establishing synergies between the different union-level actors that deal with cyber security. In June 2021, we set up the 'Cyber Security Competence Centre for Research and Industry' because research, innovation and investment are paramount for the sector to function smoothly.

GP: The best way to organize national cyber capabilities differs from one country to another depending on the political organization, on its history and on many other factors. In France, the National Cybersecurity Agency (ANSSI) was created 12 years ago with goal to have a national agency in charge of cyber, which would be neither an intelligence service nor a law enforcement team. As such, we work with many different ministries and agencies: justice, the army, intelligence services, the police, foreign affairs, economy, education. Both the Prime Minister as the head of the government and the President as the head of national defense are directly involved in cyber security and cyber defense matters. They set the priorities and allocate necessary resources. In other countries, "cyber czars" have been appointed to coordinate and represent cyber security efforts. But in France, with ANSSI being an interministerial organization, I don't believe having such a "czar" would be efficient.

Is there a good balance between cyber defense and cyber offense capabilities?

GP: In some sense, the best defense is defense: we need all the entities connected through cyber space to protect themselves, as anyone can be the entry point of a cyber-attack. But if we merely try to detect and react to the attacks, we are constantly one step behind.

At European level today, we are working to develop a framework to certify products and services from a cyber security standpoint. The European scope, which offers an attractive market to suppliers, is indeed the relevant one to protect consumers.

At the national level, it is necessary to develop both cyber intelligence and offense capabilities. In France, we have a strict separation between offense and defense, because they are too different and one should not be prioritized over the other. For the defense part, we need a cyber industry that can provide performing and state-of-the-art products and services. For the offensive capacities, it is the public sector that develops the full cyber weapons while private companies should work only on certain components. But for now, developing offense capabilities remains the realm of nation states only at both European and national levels: we are fully against counterattacks by private companies.

Beyond regulations and international frameworks, beyond defense and offense strategies, how can we make the world more resilient to cyber threats?

JL: When we go out on the streets, we adapt our behavior: we pay attention, we look left and right, we don't take unnecessary risks when driving a car or walking around. It should be the same in the cyber domain, as good defense starts with being resilient. We absolutely need to apply the principles of 'security-by-design' and 'security-by-default' not only to critical infrastructures, but also to new products and services for individual uses and to individual behaviors.

> In some sense, the best defense is defense: we need all the entities connected through cyber space to protect themselves, as anyone can be the entry point of a cyber-attack. But if we merely try to detect and react to the attacks, we are constantly one step behind.
>
> G. Poupard

Chapter 04

Insuring Cyber Risk – a Shift in Paradigm

The insurance sector is a key player in cyber risk management and the goal of cyber resilience. What is the current state of cyber insurance market? What new challenges are new technologies such as connected and autonomous vehicles bringing into the insurance business? What are the major challenges for insurers and what are the current limits they need to supersede to succeed?

The Challenges of Cyber Risk Insurance

Libby Benet

Libby Benet, JD is the Global Chief Underwriting Officer of Financial Lines at AXA XL. Libby is a Supervisory Board Member at S-RM, a global intelligence and cyber consultancy and a member of the Minnesota Lawyers Mutual Board of Directors. Libby holds a BA in Political Science from Towson University and a JD from University of Baltimore School of Law.

The digital transformation of our economies creates many opportunities but also generates ubiquitous cyber risks. Already in 2017, the OECD considered the insurance sector as a key actor to improve global cyber resilience and cyber risk management.[1] In addition, awareness of cyber risks has greatly increased in the general population, who has witnessed a rising number of attacks during the Covid-19 crisis, including critical infrastructures, such as hospitals.

> “The imbalance between supply and demand is impeding the development of the insurance sector.”

What are the challenges to cyber insurability?

Technologies that connect to the internet have not always had security as the top priority, as innovation was the first order of business. Therefore, many of the vulnerabilities introduced for companies and governments are not fully insured today. While changing, the number of governments and companies that purchase cyber insurance is still relatively low worldwide. As a result, cyber losses remain mainly uninsured today.

And indeed, there are many challenges with cyber insurability. First, the insurance sector relies on recognizing patterns in data to be able to price the product. With a natural peril for example, we have historical weather data that helps us predict what happens with a hurricane or a tsunami, while in comparison, we barely have 10-12 years of cyber insurance data. What makes the risk analysis even more complex is that the threat is man-made and constantly evolving. Additionally, there are many layers of connected and interconnected technologies, each with their own specificities, such as software, hardware, IoT, remote monitoring and so on.

When we look at accumulation modelling within cyber it is very immature. We have a couple of realistic disaster scenarios and models, but they are only a few years old and do not yet fully include changes in threat actor behavior.

[1] Enhancing the Role of Insurance in Cyber Risk Management, OECD, December 2017

> “What makes the risk analysis from an insurance perspective even more complex is that the threat is constantly evolving and that there are many layers of connected and interconnected technologies, each with their own vulnerabilities and specificities.”

Further, traditional risks such as fire and explosion and other types of property damage that are a result of a cyber event are not yet fully modelled in the industry. It’s very early days in the accumulation-modelling world.

Lack of data and issues with modelling generate uncertainty. This is an opportunity for the insurance sector, but you really need cyber security and insurance experts to come together to assess the issues and to analyze the cyber maturity of the company seeking the insurance coverage.

What are the main trends in the development of cyber insurance?

What is really new in 2021 is the outsized impact of ransomware cases, with severe losses this past year. It is changing the risk appetite of the insurance sector, which is in reactionary mode at this stage.

Another very important trend is the move from ‘silent’ to ‘affirmative’ policies, that is, being explicit about what is included and what is excluded from policies. The reinsurance community began exploring these questions around 2015-2016. AXA XL made the move in 2019, then Lloyd’s mandated insurers be explicit in their policies and giving insurers 24 months to roll out the form changes. Some in the reinsurance community are now asking their clients whether their policies are silent or affirmative. I think that this will drive the behavior of the insurance sector on all lines of business in the next year or two. This will not only affect the direct cyber products themselves but those products where cyber is a peril in other lines of business such as property or liability.

Finally, there is a growing global awareness of cyber risks and losses. Small businesses will start buying stand-alone policies covering cyber with higher limits, as opposed to insurance packages that include cyber.

However, the imbalance between supply and demand is impeding the development of the sector. Overall, there are not enough insurance companies or capacity for covering cyber risks yet. On the insurance company side, there is also a fear of the unknown in terms of shifting threat actor behavior. Additionally, there’s a limitation in accessing underwriting and risk expertise in this area. There is also a lack of maturity on the topic with key stakeholders, such as agents and brokers, who are the advisors to companies. However, there is a very strong commitment by the cyber community to improve education and awareness amongst intermediaries.

What should boards of directors know about cyber risks?

Another limitation to the development of the cyber insurance sector, is the awareness and maturity of boards of directors regarding the risk and whether they should address it through a combination of cyber security spending, self-insuring the risk or whether they want to transfer it to an insurer. Publicly traded Company Boards tend to have greater maturity than privately-owned ones but like much in cyber this too is relatively immature.

There are several things a publicly traded board should reasonably be required to know about cyber issues. Think of a three-legged stool: there are standards and frameworks, there is overall governance and finally there is the assessment of the financial harm of a risk un-addressed. The not-for-profit research by the Crossroads Group highlights the need to identify circumstances that contribute to the organization’s cyber risk, first at a local scale within an organization, and to determine the organization’s appetite for these risks.[2] This leads to the implementation of a cyber risk plan containing actions to be taken to manage cyber risk and of course to setting up oversight mechanisms.

[2] Cyber Crossroads A Global Research Collaborative on Cyber Risk Governance, Cyber Crossroads, May 2021

A Shift in Risk-Modelling Techniques for Connected and Autonomous Vehicles

David Williams

David Williams is the Managing Director of Underwriting & Technical Services, AXA Insurance UK. He has held roles such as Chief Commercial Underwriter, Reinsurance Manager, Casualty Insurance Manager, Managing Director Claims and Managing Director Underwriting. David leads AXA's work on Connected & Autonomous Vehicles, including work with five Government backed Consortia (including Venturer, UK Autodrive and Flourish). He is Chair of the ABI Autonomous Driving Insurance Group and the ABI Motor Committee, and Chair of the RISCAuthority.

> "To better manage cyber risks in the automobile sector, we need to understand how we humans interact with autonomous vehicles and how they interact with other internet-enabled devices."

All modern vehicles now include driving assistance, control units, sensors and ubiquitous internet connections. However, the future needs to be anticipated now, and it is a future of fully autonomous vehicles, connected to each other, to road services and to infrastructure.

As vehicles become more connected to their external environment, the vulnerabilities and opportunities of attacks increase dramatically, including for example threats on engine controls, tyre pressure monitoring systems or wireless key fobs. For example, in 2015, a remote attack was carried out against a Jeep Cherokee[1] through its connected entertainment channel and resulted in physical control of the braking system, amongst other elements.

The insurance industry is working hard to understand the new class of cyber risks brought by autonomous and connected vehicles. It is a big challenge, as insurance companies traditionally rely on data to price their products and provide services to their customers. Most of the data is historical data based on the performance of millions of previous policies and customers, which enables us to accurately predict overall outcomes. Today in the vehicle insurance sector, all this data comes from the operation of manual vehicles with little or no connectivity. To embrace autonomous vehicles, we need to change strategy and model the risks based on scientific understanding and modelling, rather than on data from past experience.

We need to understand how vehicles will connect and interact, as this is the entryway for any attacker, and to detail what autonomous systems and technology will be deployed, as this helps to understand the hazards incurred. For example, hacking of an automated brake system will affect not only the passengers but also very possibly, the other users of the road, whereas a dysfunctioning navigation system might drive you safely at least… but to an unwanted destination.

However, due to the volume of control modules and microprocessors, new vehicles can have around 100 million lines of code across 50 engine control units or more. In practice, there is a high probability that we ignore vulnerabilities as detailed code reviews and security evaluations are infeasible. These vulnerabilities can compromise one of the vehicle control mechanisms. For example, an attack could target the vehicle's sensor network, falsify the sensor data, or exploit control modules directly. To properly assess the vulnerabilities and manage or insure the pertaining cyber risks, we need to understand the functionality of each of the individual components, the vehicle design and the interaction between components.

Future intelligent vehicles will be increasingly connected to the internet, accept over-the-air updates, become Wi-Fi hotspots, and communicate with other internet-enabled devices such as vehicles or infrastructure. This means that the most severe security threats are still to emerge.

In addition, vehicles are also the entry point into many other vehicles and the wider infrastructure. This means that a hacker gaining physical or remote access to a vehicle can use it as a gateway to cause wider disruption. Given this possibility of physical access, simply removing internet or remote access to vehicles does not remove the risk entirely if vehicles can still connect to each other. Therefore, key security methods to protect connected and autonomous vehicles against cyber-attacks will likely be a coalition of cryptography, statistical anomaly detection systems, and software integrity solutions.

With much of this technology still being in the test phase, insurers have struggled to obtain data to run their usual risk-and-pricing models. To fill this gap, insurers now seek to embed themselves in the development work in order to gain a greater understanding of the subject. For example, the Association of British insurers has set up the 'Autonomous Driving Insurance Group' which liaises with motor manufacturers, to obtain information on new technology and to run track tests. The data and information we obtain from involvement in these areas will enable us to build analytical models, helped by AI and machine learning. This should prepare us for when these vehicles become more widely available. Connected and autonomous vehicles are a global phenomenon and sharing across borders will help to enrich this process, for example using resources like the National Vulnerability Database in the US. Practical experience can be gained at facilities such as the Thatcham Motor Vehicle Research Institute in the UK and the AXA Crash Test Centre in Switzerland.

Finally, despite a very important technological focus, many experts believe that the weakest link in terms of cyber-attacks on connected and autonomous vehicles remains the human element. User behaviors are key to issues ranging from not operating systems properly, being influenced by external communications, tampering with equipment or just not quickly installing security software updates. Awareness of user behaviors and a more balanced focus between studying the cutting-edge technologies themselves and how we interact with these technologies is necessary to ensure autonomous and connected vehicle insurability.

[1] Hackers Remotely Kill A Jeep on The Highway, Wired, July 2015

Accumulation, Dependence and Extreme Scenario Building: Preconditions for Cyber Risk Insurability

Caroline Hillairet

Caroline Hillairet is a Professor at ENSAE Paris, in charge of the actuarial program. She is a member of the Center for Research in Economics and Statistics (CREST) and the Finance and Actuarial Science Laboratory (LFA). She is a Board Member of the French Institute of Actuaries and co-director of the AXA Joint Research Initiative on the actuarial modelling of cyber risk.

Olivier Lopez

Olivier Lopez is Professor at Sorbonne University and Director of its Institute of Statistics (ISUP). He is a fully qualified member of the French Actuarial Association (Institut des Actuaires), member of its Scientific Committee, and representative member of the Education Committee of the European Actuarial Association. He is the co-director of the AXA Joint Research Initiative on the actuarial modelling of cyber risk.

Cyber-attacks have grown considerably in 2020 and 2021, in particular ransomware attacks, and this is not due to stop anytime soon. Today, most information systems are interconnected and have similar flaws, exacerbating the systemic aspect of cyber risks.

In that context, the insurability of cyber risks depends on our capacity to model cyber-attacks in a way that integrates complex dependence effects. While traditional insurance models assume that claims arrive independently, this is inadequate to model cyber events, which now tend to cluster and are correlated. Newer alternative models[1] can capture snowball effects of cyber events as well as their interactions. These models can also parameterize the characteristics of the events, so that a variety of events and their frequency can be modelled and compared, and capture shocks and persistent aftershocks that constitute 'attack contagion'.

Another major concern, aside from the frequency of cyber-attacks, is the systemic potential of a 'cyber hurricane'. In 2017, the ransomware attack Wannacry[2] led to a contagion of more than 300,000 computers over more than 150 countries. Such massive attacks may lead to many claims and induce high costs, even if each claim itself is small, and this could break the mutualization principle at the core of the insurance sector. Indeed, in such an 'accumulation' scenario, many policyholders are simultaneously victims of an attack, and a saturation of the insurer response capacity may occur, since cyber contracts generally include fast intervention of expert teams to assist the policyholder during the crisis. This incapacity of the insurance company to intervene appropriately in a short amount of time induces additional losses (financial penalties, loss of reputation, but also increased damages for the policyholders). However, there are general methodologies[3] to design accumulation scenarios, dimension insurers response capacity and help them build insurance strategies that can deal with cyber hurricanes.

In addition, even single cyber claims can have disastrous consequences. Due to the strong dependence of the economic sector on information systems, malicious attacks can generate huge damages. What statisticians call an 'extreme claim' has a significant probability to occur — as shown in the case of data leak events.[4] In such a situation, mutualization may fail, as defining the average value of a claim may not even be possible mathematically speaking, when this notion is at the core of insurance pricing.

Consequently, to make cyber insurance contracts viable, the only solution is to redesign the perimeter of insurance contracts. By introducing limits and conditions in the financial reparations, one reduces the uncertainty of the outcome for the insurer, and risk management can be performed. As extreme scenario become more prevalent, more restrictions must be added: the quality of the coverage diminishes, which is of course an issue for policyholders, and the attractiveness of the contract declines, which is an issue for the insurer, who may not attract enough customers to ensure mutualization. Understanding which factors drive the occurrence of these 'extreme' cyber claims, including for example the victim's behavior or their sector of activity, and the type of attack, is possible using data science techniques and advanced statistical tools from extreme value theory.[5] These adaptable tools can be used to draw a line between what can be insured or not, hence allow to improve the coverage by adapting it to the profile of customers.

But methodologies, even if sharp, need to be fed with proper information. One of the main challenges for cyber risk modelling and insurability currently is the critical lack of a consistent database. Solving this issue is a collective task that requires attention from insurance companies, governments, private sector, and more generally all economic agents. In this perspective, the recent study 'Lucy'[6] is a promising initiative, since it is a first attempt to provide a rigorous statistical study through collecting data from insurance brokers in France.

Insurance is based on the forecast of future events. For a risk where the behavior of the actors is so important and changes so fast, only a careful analysis of cyber events data will allow us to anticipate rather than endure.

> **"As cyber-attacks now correlate and snowball, modelling accounts for accumulation of claims and extreme cases to design resilient cyber insurance strategies."**

> **"Insurance is based on the forecast of future events. For a risk where the behavior of the actors is so important and changes so fast, only a careful analysis of cyber events data will allow us to anticipate rather than endure."**

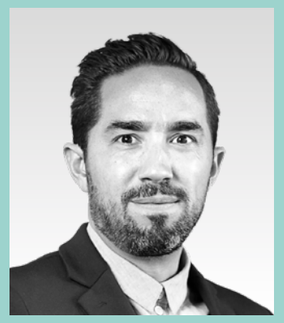
[1] Multivariate Hawkes Process for Cyber Insurance, Y. Bessy-Roland, A. Boumezoued, C. Hillairet, Annals of Actuarial Science, 2020
[2] What Is Wannacry Ransomware and Why Is It Attacking Global Computers? Alex Hern and Samuel Gibbs, The Guardian, May 12, 2017
[3] Propagation of Cyber Incidents in An Insurance Portfolio: Counting Processes Combined with Compartmental Epidemiological Models, C. Hillairet, O. Lopez, Scandinavian Actuarial Journal, 2021
[4] Heavy-Tailed Distribution of Cyber Risks, T. Maillart, D. Sornette, The European Physical Journal B, 2010
[5] Cyber Claim Analysis Through Generalized Pareto Regression Trees with Applications to Insurance Pricing and Reserving, S. Farkas, O. Lopez, M. Thomas, Insurance: Mathematics and Economics, 2021
[6] LUCY: LUmière sur la CYberassurance, AMRAE, 2021

Chapter 05

Future Scenarios and Trends

What will cyber threats be like in a decade? How can science fiction and strategic foresight help us better envision cyber resilience for tomorrow and what, according to experts, are the future regional cyber trends?

Strategic Foresight and Sci-Fi to Help Better Understand Future Threats



Olivier Desbiey

Olivier Desbiey is an Economist by training and explorer at the intersections of technology, social changes and public policy by passion. As AXA Group Senior Foresight Analyst, he scouts the horizon of emerging trends and weak signals to make sure short-term initiatives are grounded in longer-term perspective.

Current major trends suggest that digital technologies will continue to play a pivotal role in our lives. Does this necessarily mean that society will be exposed to greater cyber threats?

> “Science fiction builds a vision of future cyber issues in a manner that is complementary to more traditional forecasting tools.”

Strategic foresight considers that the potential balance of a future event depends on three aspects reflecting emerging trends and areas of uncertainty. Firstly, the current mega trends, such as geopolitical tensions or the competition between nation states and big tech companies. Secondly, the drivers of change, for example security- and privacy-by-design approaches and the increasing awareness of cyber-attacks. Thirdly, some major tensions regarding the dual use of technologies or how humans relate to technological tools.

These multiple forces could give rise to a variety of scenarios. A black swan event, with low probability and high consequences, could act as a trigger by accelerating awareness of these issues. For example, a ‘digital lockdown’ that would result from a global cyber incident could disrupt the way we currently think about the future. But for many specialists, the cyber elephant is already in the room, and some of the major challenges to come are very well illustrated… in science fiction.

Science fiction helps us build a vision of future cyber issues. Indeed, cyberpunk literature[1] and movies already dive into what cyber technologies could bring in the coming decades.

These take place in cyber space and blur the boundaries between virtual and reality. A typical breakdown of this boundary is the direct connection between the human brain and computer systems such as in The Matrix movie where the hero Neo tries to free the humans trapped in a virtual reality through cables linking their brains to intelligent machines; while the merging of human bodies with various technologies gives birth to cyborg figures, like the famous T-800 in Terminator. Some cyberpunk fictions take place in dystopic worlds where computers and internet connectivity allow for corruption, warfare between companies and against nation states, with giant multinational corporations even replacing governments as centers of political, economic or military power. In these dystopian worlds, hacker figures often appear as saviors, and contrast with the negative image of hooded hacker figures surveying the dark web that is mostly portrayed in the news today.

> “Science fiction cyberpunk literature, like climate-fiction, uses powerful narrative persuasion tools to raise awareness and help us understand what is really at stake.”

Cyberpunk provides an extreme vision of the problems we know now: the world is dominated by computer programs, cyber warfare is easier and cheaper than physical warfare, and humans can get overwhelmed by the machines they created. Sci-fi also blends in and highlights other major trends, such as pollution, climate change, overpopulation or inequalities derived from the domination of machines.

Since the Covid-19 outbreak, most foresight experts describe[2] a “world after” characterized by repeated and complex crises. This new set-up questions the way we should think about the future and emerging threats. Cyber risks crystallize this uncertainty and complexity and illustrate the limits of traditional forecasting tools where the future is projected as a logical continuity of the present. Science fiction for strategic foresight allows us to anticipate future cyber threats with ideas that regular frameworks might not otherwise imagine and helps to prepare for future scenarios and raise awareness.

Research shows[3] that climate fiction, or cli-fi, can have significant positive effects on the readers’ climate change beliefs and attitudes, including that global warming will cause more natural disasters and poverty, as well as levels of worry, perceived importance, and the perceptions that global warming will harm them personally, as well as future generations. Many of these effects can be explained by narrative persuasion mechanisms that promote a sense of identification with the story characters and immersion into the world of the story.

Science fiction authors are also called upon to imagine and describe future threats that society could be exposed to, as the French military “Red Team”,[4] made of sci-fi authors, exemplifies. Their mission is to provide out-of-the-box thinking and to come up with disruptive scenarios that anticipate how terrorist groups or hostile states might use advanced cyber technology in the future for example.

Disruptive scenarios and storytelling tools can help shift beliefs and attitudes regarding science and environmental issues, raise awareness and anticipate future threats we need to prepare for, now. The following article aims to do just that.

[1] Science Fiction in the Eighties, Gardner R. Dozois, The Washington Post, December 30, 1984
[2] 2020 Strategic Foresight Report, Charting the Course Towards A More Resilient Europe, European Commission, 2020
[3] Reading Environmental Literature Can Persuade on Climate, Gustavson et al., Yale Program on Climate Change Communication, 2020
[4] The French Army is Hiring Science Fiction Writers to Imagine Future Threats, Andrew Liptak, The Verge, July 24, 2019

Anticipating the Future of Cyber-Attacks: Tales from the Future and Real-Life Points of Caution

Cécile Wendling

Dr Cécile Wendling is Group Head of Security Strategy and Awareness at AXA. Prior to this position, she was Group Head of Foresight at AXA and Associate Researcher at Centre de Sociologie des Organisations (CNRS — Sciences Po Paris) in sociology of risks and catastrophes. She has a PhD from the European University Institute on EU crisis management and gives lectures on foresight methods, risk and crisis management, among others.

Mathieu Cousin

Mathieu Cousin is leading the Threat Anticipation activities at AXA Group Security since the 1st January 2020. Before joining AXA Group Security in August 2016 as Security Researcher in the Strategy, Architecture and Research team, Mathieu spent four years as a research analyst and security researcher.

Lou-Anne Ducos

Lou-Anne Ducos is a Master student from Sciences Po Saint-Germain-en-Laye studying international relations and a security analyst intern for the threat anticipation team at AXA Group Security since March 2021.

‘Fake news of a hack endangers multinational, social media blamed now under governmental control”

December 4. 2023

Sitting in your open space, you try to finish your missions as fast as you can before picking up your kids from school. But you find it impossible to concentrate. Phones buzz, everyone whispers, it looks like a playground. Annoyed, you decide to go home to finish your work and you meet one of your colleagues on the way: ‘Have you heard the news?’, they ask. You have absolutely no idea of what he is talking about, but after finally checking your phone, everything becomes clear: Facebook, Instagram, Twitter, TikTok abuzz about your company.

A well-known cybercriminal group announced it hacked your system and claims to have access to all the information on your customers, distributing samples on social media to prove it. The hackers gave you 24 hours to pay the ransom before they publicly release all the information in their possession. This is a nightmare: you spent the past six months working on a big merger and acquisition, and, with the green light given by the regulator, the game-changing deal for the nation’s economy was almost done. The company knows about cyber-attacks and should be prepared against it, especially in these important times. Irritated, you decide to get more information. Your leadership is unanimous: the company is not experiencing any cyber-attack – the news is fake. Relieved, you think that the public affairs department just has to claim the truth.

But it is already too late, and the share price of the organization is dropping. The first official response stating that “The company is investigating any possible breach” and the second, claiming that the “samples” spread by hackers were fake information, go unnoticed. No one is listening, and fear wins over reason, but when the ransom deadline is over and the hackers take no retaliation actions, everybody finally realizes it was a lie. But the affair has become a huge cost to the company and your merger and acquisition is compromised.

The government that was supporting you in this merger and acquisition process decides that such a series of events will not happen again. As a first step, all social media will face restrictive measures to prevent such a situation from being repeated and many users see their accounts closed without notice. While you understand the reason beneath this stricter control, you fall asleep thinking of the future of your freedom of speech.

In real life

This scenario could already happen now, and might come true in the months and years to come. Indeed, disinformation is a growing concern for both public and private actors. Europol defines social media as increasing “the proliferation of disinformation and conspiracy theories”.[1] As an example, recent Russian cyber-attacks to meddle in the U.S. elections using social media[2] highlight the growing influence these platforms can have on people’s opinions and behaviors. Moreover, cyber-attacks entail significant indirect or soft costs beyond direct costs, (e.g., brand erosion, loss of confidence from customers, partners and investors). Since 2016, the Ponemon Institute global survey of data breaches found the average cost of reputational damage to represent more than 40 percent of all costs.[3]

To limit the impact of fake news, reputational risk is becoming an integral part of strategy and planning. It can include for example the monitoring of social media to quickly detect any attempts of disinformation, the preparation of a communication plan, including a centralized control over all your communication channels and means for the public and the press to check official messages and statements.

Fake news also affects individuals with different and varied consequences. Awareness is one of the key tools so far.

[1] EU Terrorism Situation and Trend Report 2021, page 28, Europol, 2021
[2] Russia Used Social Media for Widespread Meddling in U.S. Politics: Reports, Mark Hosenball, Reuters, December 17, 2018
[3] Calculating the Reputational Cost of Cyber Security Breaches, Barclay Simpson, April 26, 2016

‘Climate change shuts down the health care system in the whole country’

September 15. 2022

45 minutes has passed since you arrived in your doctor’s waiting room. You already had time to read all the magazines available and decide to take your phone to check the latest news. Social protestations against labor reforms… slow economic growth… you finally opt for an article on natural disasters. Massive fires are burning down entire buildings in the West, flooding was followed by a devastating hurricane in the East. Nothing very surprising, you think, as climate change is causing important damages everywhere.

Your doctor finally arrives, and your medical consultation begins. Quickly, you feel that your doctor is irritated. He explains to you that since this morning, none of his records are available and that the entire medical system is down. ‘How is that even possible?’, you ask, and he starts talking about natural disasters and data centers. At one point, you stop him as you really struggle to see the link between natural disasters and the loss of your medical data. He asks you if you’ve heard about the fires in the South West and the recent hurricane in the Eastern coast, and you explained proudly that you have indeed just read this detailed article on infrastructures damaged throughout the country. However, what you were not expecting is that among these infrastructures, some crucial data centers were destroyed, preventing part of the country from accessing medical data; and for the first time, you realize how dependent on physical structures our digital world is.

While this incident was minor for you, you cannot stop thinking about people in urgent care and the devastating consequences a fire can have on them and their medical teams. What are we going to do if all our critical activities can be brought offline at any time because of physical incidents?

‘Hackers and their home-made AI make off with millions in major cyber bank robbery’

June 21. 2028

Nothing destined you to this path, but an economic crisis, disillusion and the necessity to provide for your family made this job an opportunity you could not miss. When your friend told you about this opportunity, you declined, thinking that you had none of the computer science abilities required for this kind of job, but he promised it would be easy and he was right. You now make more money than you ever thought you would, just by launching cyber-attacks on wealthy companies.

Thanks to artificial intelligence, cyber-attacks are automated, and the level of skills required to launch them is quite low. Some guys you met on the dark web gave you appropriate tools to work with. You are part of a team of 30 people, each of you with your own specialty, and you barely notice the difference with your previous job. Today, your mission is to use a powerful AI tool against a banking company. You know that you are going to face their ‘Endpoint Detection and Response’ solution, which is in theory able to detect threats directly on information systems, but it does not matter, your tool is smart enough to bypass it. It quickly detects a large number of computer security flaws unnoticed by the software publisher or service provider, the so-called ‘zero-days’, and lets you pick and exploit them, rendering the bank protection systems useless. Your AI also accelerates your attacks thanks to automation, so you can go home early most days.

In real life

This scenario could already have happened, and might happen in the months and years to come. Critical infrastructures are threatened by malicious attacks, such as the ransomware attacks launched in May 2021 against one of the U.S. largest pipelines[4] and the Irish health services[5], and are physically threatened by the consequences of climate change. The increased number of natural disasters pushed the Information Security Forum (ISF) to identify “a major disruption and damage to IT systems and assets after a natural disaster” as a major threat for 2022.[6] As such, cases of outage and attacks against critical infrastructures, including cyber and interconnected ones, are going to become more frequent and should be carefully mitigated.

Aside from taking proactive measures to fight climate change globally, critical infrastructure management and their users can limit the impact of cyber and natural risks by securing remote access, using for example endpoint protection, good password hygiene and security practices, or by having an updated and accurate inventory of assets and monitoring for anomalies. Data could be duplicated and stored in different locations to avoid data loss such as for the OVHcloud services firm fire in France in March 2021.[7]

In real life

This scenario could happen in the upcoming months and years, as AI-powered attacks can also take many forms, from designing an attack, providing extreme speed of compromise, to mimicking expected communications and masking on-going attacks.

AI also offers surveillance tools against cyber-attacks, from scanning and analysis to response automation to contain a cyber-attack quickly. Continuously improving cyber security systems and scanning for existing vulnerabilities also contributes to limiting the impact of AI-based attacks. Currently, cyber ecosystems are being put in place across economic sectors or economic chains and facilitate the sharing of information relative to attacks.

All you have to do is to launch the attack and artificial intelligence will do the rest. AI versus AI, your attack went successful. You found five different vulnerabilities that will be used to steal data, resell it or use it to launch new cyber-attacks. You would never have believed that data would make you rich, but well it definitely became the new oil!

‘Quantum-based cyber-attack crushes car company hopes for market domination – ‘absurdly unprepared’, experts say’

November 5. 2031

Tomorrow is a big day for your tech team, as the company is launching a new series of cars with ground-breaking technologies that none of your competitors master. After years of work, it is time to celebrate, and you joke with your colleagues about the millions you are going to make. Nothing could spoil your joy today.

However, one of your colleagues runs to you, as the CEO needs to talk to you urgently: your main challenger just announced his new collection of cars similar in every way to yours. You cannot believe it, as you have been working in the uppermost secrecy for the last 15 years to develop these technologies. How could they have developed the exact same model, and to have it ready one day before you launch your own collection? The tech news alerts accumulate on your phone and you have to accept the reality. Furious, you call your staff: ‘We have been spied on! How did you let that happen?’

Surprised, one of your employees explains that all confidential information has been encrypted following the procedure. At the back, a young intern in the IT department seems embarrassed. You ask him what he thinks about the situation and he explains how the government of your competitor may have been able to break your cryptographic protocols and algorithms using quantum computing. He continues saying he was quite surprised at the beginning of his internship when he realized that you were not using any data encryption solution resistant to quantum technology.

You now realize that you have indeed heard about a quantum-proof encryption algorithm a few months back, but it was very expensive and you had not expected quantum technology to become a threat before a couple of decades at least. A couple of years back, the data center of your IT provider had been robbed, and amongst the many physical servers’ stole were several of yours. Thanks to backup data centers, allowing you to duplicate data and locate it elsewhere, it had not affected your operations and, at the time, investigators and consultants had assured you that it would take about 100 years for anyone to decrypt the stolen data. By believing these assessments, you’ve made one error that now costs you 15 years of work and the first player advantage.

In real life

All experts do not agree about when the various approaches covered in the field of ‘quantum computing’ will be mature enough for public uses[8,9,10], but quantum computing technology could come to fruition as early as within the next 10 years. The important consequences of quantum computing on cyber security require getting ready now. Indeed, some currently secure algorithms and quantum computers could break cryptographic protocols with reasonable time and effort. Moreover, it is likely that large numbers of organizations, from governments to criminal groups, are currently storing encrypted data that they have intercepted with the will to break the encryption later.

However, quantum technologies also offer progress in cyber security using post-quantum cryptography and physical quantum security. Engaging in a transition towards more quantum resilient-encryption and monitoring all data breaches that could be used against the organization if decrypted could help mitigate the quantum risk.

[4] Pipeline Attack Yields Urgent Lessons About U.S. Cyber Security, The New York Times, May 14, 2021
[5] Irish Cyber-Attack: Hackers Bail Out Irish Health Service for Free, BBC, May 21, 2021
[6] Threat Horizon 2022: Digital and Physical Worlds Collide, ISF
[7] Millions of Websites Offline After Fire at French Cloud Services Firm, Reuters, March 10, 2021
[8] When Will Quantum Computers Impact Our Day-To-Day? Gary Fowler, Forbes, April 28, 2021
[9] A Quantum Computing Future is Unlikely, due to Random Hardware Errors, Subhash Kak, The Conversation, December 3, 2019
[10] When Will Quantum Computers Be Consumer Products? Christianna Reedy, Futurism, July 31, 2017

Around the World in Future Cyber Trends

... Asia

Dale Johnstone, Chief Security Officer, AXA China Region Insurance Company Limited, AXA General Insurance Hong Kong Limited

'Over the coming few years, expect to see the bad actors continue to mature and to target more Asian based organizations. Asian culture often tends to be more reactive focused — where an incident occurs, the ability to respond effectively is very efficient — rather than having a strong focus on being strategic and focusing on the overall information security management approach to plan, anticipate and hopefully avoid being breached in the first place. Now, the gap is closing.'

Numbers: 'Since 2019, cyber criminals have shifted from indiscriminate, opportunistic attacks, to more targeted 'Big Game hunting', i.e. targeting large businesses with high value data or assets in hope of a higher ransom pay-out. This has been observed globally. In Singapore, while most of the cases reported were from SMEs, ransomware operators were observed to target larger assets in the manufacturing, retail and healthcare sectors between May and August 2020.' (Source: Global and Local Ransomware Trends 2020 Q1-Q3, Singapore Computer Emergency Response Team, Nov 17, 2020)

... the US

Libby Benet, Global Chief Underwriting Officer of Financial Lines, AXA XL

'The Biden administration issued an executive order in early May 2021 that is particularly helpful, about the software industry working more diligently to secure their software. In the near future, I expect we will see more on the topic from this administration and from governments around the world. I would look for governments to first compel software providers to secure their software, and if they don't demonstrate that they can police themselves, I think we'll see regulations that will require that security be in place, and in the hardware area as well.'

'The calls of the security community are now being heard in the halls of power and by governments around the world. The insurance sector is the canary in the coalmine, as we can quantify the costs of the loss, which makes it real to everybody. But we have gone into the geopolitical arena now, and we need a massive global response to these criminal gangs via collective law enforcement.'

Numbers: 'In the first half of 2020, researchers observed a marked seven-fold jump in the number of ransomware attacks reported globally, while ransomware accounted for almost half of all cyber insurance claims filed in North America.' (Source: Global and Local Ransomware Trends 2020 Q1-Q3, Singapore Computer Emergency Response Team, Nov 17, 2020)

... France

Guillaume Poupard, General Director, National Cyber Security Agency of France (ANSSI)

'In the next months and years, a most interesting topic will be cyber sovereignty, a very complex and political topic. Will Europe be able to stand firm that we only want European rules to apply to our critical systems and data, that we can have external partners and allies without accepting their own rules and laws? If we can do this while remaining open, as sovereignty doesn't mean protectionism, it will be very interesting.'

Laurence Lemerle, Head of Engineering and Cyber Risks, AXA France

'Companies now evolve very rapidly: they have become aware of the risks and look for solutions. They now understand that the first step is to equip themselves with cyber defense solutions, and then insurance. There is still some explaining to do, in particular towards SMEs, but things are moving fast and this is encouraging.'

Numbers: 57% of French companies have seen at least one cyber-attack in 2020 (Source: 6e édition du baromètre annuel du CESIN, CESIN, February 9, 2021); the French Agency for the security of information systems (ANSSI) received 255% more reports regarding ransomware attacks in 2020 than in 2019 (Source: Rapport menaces et incidents du CERT-FR, ANSSI, February 5, 2021)

... the UK

Heyrick Bond Gunning, CEO, S-RM

'Scarcity of talent, GDPR fines and the likely withdrawal of cyber ransom insurance are offset by innovative cyber response services and the emergence of a new talent pool from more backgrounds outside the traditional IT, who bring diversity and complementary to the workforce.'

Numbers: 'Despite COVID-19, cyber security remains a priority among management boards. […] 77% of businesses say that cyber security is a high priority for their directors or senior managers' (vs. 69% in 2016). 'But COVID-19 has made cyber security harder […] With resources stretched, fewer businesses […] report having up-to-date malware protection (83%, vs. 88% in 2020) and network firewalls (78%, vs. 83% in 2020)' (Source: Cyber Security Breaches Survey 2021, GOV.UK, March 24, 2021)

... Europe

Heyrick Bond Gunning, CEO, S-RM

'Something is really new: cyber used to be a domain where people used to remain in their corner and avoid talking to each other as they considered it a security risk. Now it has changed dramatically and everybody understands that they can be successful only if others help them. This gives me a more optimistic outlook: we as a group of people and of nations are much stronger to deal with threats than we were before.'

'The gloomy picture of inevitable growing cyber-attacks and related costs — as it is definitely going to get worse — is counterbalanced by the various steps Europe has taken regarding policy and regulatory framework, investment frameworks, in building capabilities, developing standards that help the market to go in the right direction and in building up collaboration networks between the different actors.'

Numbers: 'The annual cost of cyber-crime globally in 2021 was $5.5 trillion USD.' […] 'In 2020, there were 949 significant malicious attacks in the EU, of which 742 targeted critical sectors (energy, transport, water, health, digital infrastructure and finance sector). That is a 72-percent increase compared to 2019.' (Source: EU Creates New Cyber Unit, After Wave Of Online Attacks, Elena Sánchez Nicolás, euobserver, June 24, 2021)

crédits photos : Shutterstock