VOLUME 5 (2019) ISSUE 1

European Cybersecurity Journal

Strategic perspectives on cybersecurity management and public policies

Interview with Steven Wilson

Information Sharing for the Mitigation of Hostile Activity in Cyberspace

The consequences of the (extra)territorial scope of the GDPR

ANALYSES • POLICY REVIEWS • OPINIONS

THE KOSCIUSZKO INSTITUTE

European Cybersecurity Journal

Strategic perspectives on cybersecurity management and public policies

The European Cybersecurity Journal (ECJ) is a specialised publication devoted to cybersecurity. The main goal of the Journal is to provide concrete policy recommendations for European decision-makers and raise awareness on both issues and problem-solving instruments.

Editorial Board

Chief Editor:

Executive Editors:

Honorary Members Of The Editorial Board:

Members Of The Editorial Board:

Associate Editors:

Design & DTP:

Joanna Świerad-Solińska

Proofreading:

Adam Ladziński, Justyna Kruk

ISSN: 2450-21113

Citations: This journal should be cited as follows:
”European Cybersecurity Journal”
Volume 5 (2019) Issue 1, page reference

THE KOSCIUSZKO INSTITUTE

Published by:
The Kosciuszko Institute
ul. Feldmana 4/9-10
31-130 Kraków

Phone: 00 48 12 632 97 24
E-mail: editor@cybersecforum.eu

Printed in Poland

Disclaimer: The views expressed in articles are the authors' and not necessarily those of the Kosciuszko Institute. Authors may have consulting or other business relationships with the companies they discuss.

Contents

Editorial

Barbara Sztokfisz

Chief Editor of the European Cybersecuirty Journal

Dear readers,

It is my great honour and privilege to present you the new issue of the European Cybersecurity Journal. This edition coincides with a huge milestone for the CYBERSEC family of events. In the first quarter of 2019, CYBERSEC is travelling to Brussels, for the second year in a row, to meet high-level European decision-makers. It will then set off across the Atlantic to Washington, D.C., to tackle digital challenges and advance cybersecurity around the globe.

The year 2019 will certainly be marked by new, challenging and decisive political activities that will affect us all. We will be able to verify how unwavering our trust is in critical processes shaping our democracies and economies in the era of increasing digital turmoil. The upcoming European Parliament elections as well as the presidential elections in Ukraine and other CEE countries are only a few examples of 2019 political highlights that will put the level of resilience of electoral processes in Europe and the overall preparedness of democracies for cyber-enabled threats to the test. Online manipulation and disinformation campaigns jeopardise election outcomes, create confusion and plant a seed of distrust in electors' minds. "Elections belong to the people. It's their decision", stated Abraham Lincoln, and should remain so.

It is worth emphasizing that each year a lot is done to make our cyber world safer and more stable: the entry into force of the NIS Directive and the GDPR regulation in 2018, the advanced work on the Cybersecurity Act, ePrivacy Regulation, the revision of Open Data Directive (PSI) and the ever deeper discussions on the latest technological challenges such as 5G, blockchain, Artificial Intelligence or High Performance Computing. But we still have a lot more to do together. At CYBERSEC 2018, the distinguished conference speakers said with one voice: we need trust, we need tools to provide it, and we need to be agile and less hesitant to act. This statement has never been truer than today.

I sincerely hope that this publication will contribute to boosting our cybersecurity preparedness, taking us closer to securing the world's digital DNA.

I extend to you my best wishes for 2019! I hope this year we see accelerated efforts to advance the quest for cyber trust and cybersecurity in general.

Enjoy the read!

Barbara Sztokfisz

CYBERSEC

EUROPEAN
CYBERSECURITY FORUM

SAVE THE DATE
FOR OUR 5th ANNIVERSARY

29-30.10.2019

SECURING THE WORLD'S DIGITAL DNA

Confronting cybercrimes in the digital age

Interview with Mr Steven Wilson, Head of the Cybercrime Center at EUROPOL

Steven Wilson originates from Ayrshire, Scotland. He was a Police Officer in Scotland from 1985-2015. During this time, he served with Strathclyde Police, Scottish Crime and Drug Enforcement Agency, Her Majesty's Inspectorate of Constabulary and, since 2013, with the reorganisation of policing in Scotland into a national force, Police Scotland.

Steven performed a variety of senior Detective roles and was responsible for the national units in Scotland delivering: witness protection, covert technical policing, fugitives, undercover policing, assisting offender programme and all forms of cybercrime and cyber enabled crime including online child protection.

Steven was the Scottish representative on UK cyber governmental and policing groups and led on industry and academic partnership groups on cyber resilience in Scotland.

Steven has also worked in covert policing, major investigations, sex offender management, Counter Terrorism investigations and represented the UK on International policing matters.

Steven commenced as Head of EC3 on 18 January 2016.

Thank you, Sir, for finding time for this interview. The European Cybercrime Centre (EC3) was set up by Europol in 2013. How has its role changed from that time? What major shifts in the cyber-threat landscape did you observe over the past few years? Taking into account the increasing degree of digitisation of economies, does EC3 record the growing importance of crimes taking place in cyberspace?

The last years have shown us that cybercrime continues to evolve and mature. Not only using known modi operandi but also taking new forms and directions, cybercrime continues to increase in terms of scope, volume, and damage, as demonstrated in some of the more recent attacks of unprecedented scale. These developments emphasise the importance of EC3's goal – to strengthen law enforcement's response to cybercrime and protect European citizens and organisations from online crime.

Since its establishment, EC3 has made a significant contribution to the fight against cybercrime: it has been involved in tens of high-profile operations and hundreds of on-the-spot operational-support deployments resulting in hundreds of arrests. Furthermore, EC3 has analysed hundreds of thousands of files, the vast majority of which have proven to be malicious.

Not only using known modi operandi but also taking new forms and directions, cybercrime continues to increase in terms of scope, volume, and damage, as demonstrated in some of the more recent attacks of unprecedented scale.

Each year, EC3 reports on key findings and emerging threats and developments in cybercrime in its flagship strategic report, the Internet Organised Crime Threat Assessment (IOCTA). Among other things, a growing use of anonymisation and encryption tools by cybercriminals was reported. This renders many traditional investigative techniques ineffective, and often negates the possibilities of digital forensic analysis.

Ransomware

The threat of ransomware has been significantly increasing over the last years. By 2017 the number of ransomware families had exploded, their impact overshadowing other malware threats such as banking Trojans. Ransomware damages increased fifteen-fold from 2015 to 2017. Even though ransomware has stabilised, it has done so at a high level and it still remains the dominant threat according to the input we received for the IOCTA.

The threat of ransomware has been significantly increasing over the last years. By 2017 the number of ransomware families had exploded, their impact overshadowing other malware threats such as banking Trojans. Ransomware damages increased fifteen-fold from 2015 to 2017.

DDoS

Criminals continue to use Distributed-Denial-of-Service (DDoS) attacks, making them a consistent and growing threat. It is not only one of the most frequent attacks, but it is also becoming more accessible, low-cost and low-risk for criminals.

In April 2018, four administrators of the DDoS marketplace webstresser.org were arrested as part of a complex investigation called Operation Power Off. The Dutch Police and the British National Crime Agency led the investigation, with support of Europol and a dozen law enforcement agencies (LEA) from around the world. The website – where users could pay as little as 15 euros a month to rent out stressers and booters to carry out crippling DDoS attacks – was shut down. This resulted in a 60% decrease in DDoS attacks across Europe. Webstresser.org was considered the world's biggest marketplace to hire DDoS services, with over 136 000 registered users and 4 million attacks measured by April 2018.

CSE

The threats related to online child sexual abuse have stayed relatively stable. Online sexual coercion and extortion have remained a key threat during the last few years. Live streaming of child sexual abuse has now become an established threat. Offenders are continuing to improve their operational security, making law enforcement agencies' investigations more difficult.

Darknet marketplaces

Darknet markets have been in the LEA and public spotlight since the takedown of Silk Road. Providing easy access to a wide range of illicit commodities and services, these markets are key enablers for other crimes. Since Silk Road, multiple Darknet markets were taken down. In 2017, Europol was involved in actions to disrupt two of the largest Dark Web marketplaces, Hansa and AlphaBay.

Social engineering

The significance of social engineering within both cyber-dependent and cyber-enabled crime continues to grow. Social engineering can take many forms. Phishing via email is still the most frequent form. This typically involves victims unwittingly installing malware by opening a malicious email attachment or following a link to a malicious website. This can also be done by phone (vishing) and SMS (smishing).

The significance of social engineering within both cyber-dependent and cyber--enabled crime continues to grow. Social engineering can take many forms. Phishing via email is still the most frequent form.

Classic forms of social engineering involve convincing victims to divulge information or act abnormally. Romance scams commonly take place on online dating websites, with scammers using social media or email to make contact. The scammer feigns romantic intention towards the victim to gain their affection. They then tell an elaborate story and ask the victim for money, gifts, or bank account/credit card details. Together with technical support scams (often referred to as Microsoft support scams) and advanced fee fraud, these classic forms still feature prominently in law enforcement reporting and still result in significant financial and emotional damage to their victims.

The financial sector highlighted CEO/business email compromise (BEC) fraud as a key threat in this year's IOCTA. Attackers impersonate a high-ranking individual within a company in order to initiate fraudulent payments. This kind of fraud can result in significant losses and in some cases has even resulted in bankruptcy for the affected company. Many social engineering scams targeting EU citizens are now being carried out by West African organised crime groups (OCGs). While in 2013 few people had heard of cryptocurrencies, their use has now become mainstream. Not only are cryptocurrencies exploited by cybercriminals, businesses and users of cryptocurrencies are now targets of cyber-attacks, which historically targeted traditional financial instruments.

While in 2013 few people had heard of cryptocurrencies, their use has now become mainstream. Not only are cryptocurrencies exploited by cybercriminals, businesses and users of cryptocurrencies are now targets of cyber-attacks, which historically targeted traditional financial instruments.

Now, let's move to the future – what is cybercrime going to look like? Which technologies and methods of attacks, in your opinion, are going to be the most popular among cybercriminals? Which of them can be of particular danger for the cyber ecosystem as a whole?

Cyberattacks will become increasingly stealthy and harder to detect. As reported in the IOCTA 2018, mobile malware in particular is likely to increase, as mobile banking is overtaking online banking. Insecure Internet of Things (IoT) devices pose a significant threat. The Mirai attack was one of the first prominent examples of the criminal abuse of IoT devices, creating one of the largest DDoS attacks at the time. In 2016, the malware took advantage of poorly protected IoT devices, having no or default passwords. With estimates of something like 20 billion of IOT devices by 2020, this is a major concern.

Artificial Intelligence

Artificial Intelligence (AI) will continue to develop and pose new challenges. AI systems are now able to generate synthetic images, text, and audio. Criminals could misuse these abilities to impersonate others online. However, AI also opens up new possibilities for LEA. The promise offered by big data and machine learning can open up a wealth of opportunity to facilitate a more proactive approach towards crime fighting. This will be a key part of EC3's development strategy as we move into the years to come.

Critical infrastructure

WannaCry and NotPetya gave us a view of what a global cybercrime attack destabilising Critical National Infrastructure could look like, and unfortunately it is likely to happen again. The repeated attacks on the Ukrainian power grid and the DDoS attacks on ISPs crippling train networks in Sweden are examples of how this could develop. Because Europe both has an advanced economy which is heavily technology dependent and holds an important geopolitical position, it is a prime target for such attacks.

What are main motivations of cybercriminals? Is financial profit actually the most important incentive for them? Or maybe sometimes it is not about money? What about state-sponsored cyberattacks or the ones that aim to gain information and conduct industrial espionage?

The threat landscape faced by Europe in cyberspace is diverse. In terms of the type of threats as well as the actors behind them. There is a narrowing of the gap or even an overlap between serious organised crime, 'script kiddies' and nation-state attacks. This is facilitated and underpinned by a growing crime-as-a-service model that interconnects specialist providers of cybercrime tools and services with an increasing number of organised crime and other actor groups. This not only enables cyberattacks that may misrepresent the technical capability of the actors involved but also further complicates attribution. Both state and non-state actors, after all, can use tools from the same toolbox.

So when we speak of ransomware retaining its dominance and social engineering functioning as the engine for many cybercrimes, this cuts across the different actors. Ransomware is a prime example of this. Whilst it primarily appears to be a crime focused on financial gain, it can also lead to disruption and this may, in fact, be the motive of the perpetrator.

> **The threat landscape faced by Europe in cyberspace is diverse. In terms of the type of threats as well as the actors behind them.**

Main motivations for cybercriminals depend on the type of actor. We can speak of cybercriminals who carry out their attacks for financial gain, but at the same time certain cybercriminals are more focused on disruption or showing off their skills. The increasing convergence of criminality makes it more complex to distinguish between actors. Different parties have distinct motives, but they may not be so easily identified. And among those different actors, criminals are our focus, where state actors fall within the remit of intelligence services.

When a cybercrime occurs, however, we are often left with little concrete evidence to attribute it to a specific threat actor. As we find ourselves in the dark about the origins of the perpetrators, our primary objective remains to support our Member States in the investigation of the cross-border crimes they face and to ensure we are the linking pin in coordinating the law enforcement response.

Much of the cybercrime we face is primarily financially driven, especially since this falls within our domain. There are other developments which are receiving an increasing amount of attention, but they are generally not part of our mandate. This includes influencing the public through fake news.

Could you describe the cooperation of Europol with the industry? What is the type of companies or institutions that Europol cooperates with? Do they represent specific sectors? Have you noticed in recent years any changes in their approach when it comes to the willingness to share the information?

While different societal actors play distinct roles in the cybersecurity ecosystem, cooperation between these different groups remains crucial, since each actor may have a different piece of the puzzle.

Many of the operations coordinated and supported by Europol demonstrate how the knowledge, experience, and information held by a variety of public and private parties are indispensable to engage in the successful disruption of criminal processes.

We cooperate with important actors in the private industry. In 2013 EC3 identified the need for establishing Advisory Groups to provide guidance, bring expertise together, and strengthen practical cooperation between LEA and key domains. In 2013 it established Advisory Groups in the areas of Financial Services and Internet Security. In 2015 EC3 added a group on Communication Providers. The members are recruited from experts operating in these respective sectors (for example: McAfee, Mastercard, Vodafone). In November 2018 meetings took place with the three Advisory Groups.

The general impression is that companies are more willing to exchange knowledge and experiences and work together.

Many of the operations coordinated and supported by Europol demonstrate how the knowledge, experience, and information held by a variety of public and private parties are indispensable to engage in the successful disruption of criminal processes.

For example, the European Money Mule Action (EMMA) – which had its fourth iteration in 2018, which ran for 3 months – bringing together information from both the financial services sector and law enforcement. Europol, along with Eurojust, provided a coordinating role to facilitate the real-time cross-checks against Europol's databases of data gathered during the operations, and to collect intelligence for further analysis as well as swiftly forward and facilitate the execution of European Investigation Orders. More than 300 global financial institutions were involved in this coordinated operation resulting in the arrest of 140 money mule organisers and the identification of 1500 money mules.

One of the most noteworthy areas of cooperation is the No More Ransom (NMR) initiative at nomoreransom.org – a joint endeavour between law enforcement and industry – with the goal to help victims of ransomware retrieve their encrypted data without having to pay the criminals.

The project has more than 130 partners, and currently helps the public by providing not only prevention advice but also victim mitigation by giving free access to over 50 different tools to decrypt their data. More than 40 000 people and organisations worldwide have had their encrypted files restored as a result of this service.

Our most recent success within NMR was with regard to the most aggressive form of ransomware named GandCrab. Within the first 24 hours of making the decryption tool available, 600 victims were able to release their files.

The complexity of cybercrime continuously requires us to adapt, a key aspect of which is to further strengthen existing partnerships and to identify new partners to cooperate with and new ways of structuring these partnerships.

This is particularly relevant, for example, in the case of our enhanced investment in developing and supporting the development of capacity with respect to virtual currency investigations.

At Europol, we have developed good partnerships with virtual currencies exchanges to ensure we can offer Member States the support they need.

> **The complexity of cybercrime continuously requires us to adapt, a key aspect of which is to further strengthen existing partnerships and to identify new partners to cooperate with and new ways of structuring these partnerships.**

Do you see the role of white hat hackers as important in the fight against cybercrime? What are other entities that are important in the overall process of ensuring the proper level of cybersecurity?

White hat hackers play a role in the identification of vulnerabilities and the improvement of the robustness of software. This is, however, more focused on cybersecurity, although we do recognise it could have an impact on cybercrime as well when vulnerabilities are discovered and patched within a reasonable time frame to prevent cybercriminals from taking advantage of them.

EC3 has partnerships with several important actors in the process of ensuring cybersecurity. In May 2018, Europol signed a Memorandum of Understanding (MoU) together with the European Union Agency for Network and Information Security (ENISA), the European Defence Agency (EDA), and the Computer Emergency Response Team for the EU Institutions, Agencies and Bodies (CERT-EU) to establish a cooperation framework between their organisations. The MoU aims at leveraging synergies between the four organisations, promoting cooperation on cybersecurity and cyber defence, and is a testament to the trusted partnership that exists between these EU agencies.

Legislation is also an important part of providing cybersecurity. Among initiatives to improve EU cyber-resilience, the European Commission put forward a legislative proposal of an EU certification framework for ICT security products and services. The certification will demonstrate that ICT products comply with specified security requirements, making it easier for users to have confidence in the security of these products.

The influence of the users themselves on cybersecurity should not be underestimated. The human factor plays a major role in making businesses vulnerable for cyberattacks. Employees are often uninformed, putting businesses at risk. Research shows that careless or uninformed staff is the second most likely cause of serious security breaches in businesses, second only to malware. This shows it is important to train people to protect themselves. EC3 also plays a role in informing the public. This includes the provision of high-quality, pan-European prevention and awareness campaigns and activities, often in close cooperation with industry partners.

What should the international cooperation look like? At the transatlantic level – what will be the consequences of the CLOUD (Clarifying Lawful Overseas Use of Data) Act in practice? And at the EU level – is the 'Proposal for a Regulation on European Production and Preservation Orders for electronic evidence in criminal matters' a step forward in ensuring effective investigation and prosecution of crimes? What should the access to e-evidence across borders and public-private cooperation look like? How can we prepare law enforcement agencies and the judiciary to counteract these processes?

Crimes committed with a cyber component are inherently transnational and therefore illustrate the necessity for international cooperation. Within the cybersecurity ecosystem, the European Cybercrime Centre (EC3) fulfils through its very nature a unique role in the fight against cybercrime. Due to its ability to act as a coordinating and supporting platform, EC3 brings both people and information together to enable the Member States in cooperation with various partners to carry out critical operations.

Concerning the consequences of the CLOUD Act and the Proposal for a Regulation on European Production and Preservation Orders for electronic evidence in criminal matters, the availability of electronic evidence is crucial in any cross-border investigation (and not limited to cyber cases). Its importance will continue to increase considering the ever-growing digitalisation of communication.

Crimes committed with acyber component are inherently transnational and therefore illustrate the necessity for international cooperation.

For Europol, the importance of the matter cannot be underestimated as Europol's business model relies on the availability of up-to-date evidence, purpose-fit for use in courts. From Europol's perspective, a Union-level agreement would be preferable compared to a fragmented legal landscape. It is too early to define a possible role for Europol in this context until the deliberations at the political level provide for more clarity. Europol stands ready to support EU efforts in exchanging electronic evidence. The technical infrastructure and expertise already available at Europol could facilitate EU cooperation with the US if this was deemed legally feasible and considered appropriate by our stakeholders.

And last but not least, to summarise, what would you say is the single biggest challenge the law enforcement entities face right now?

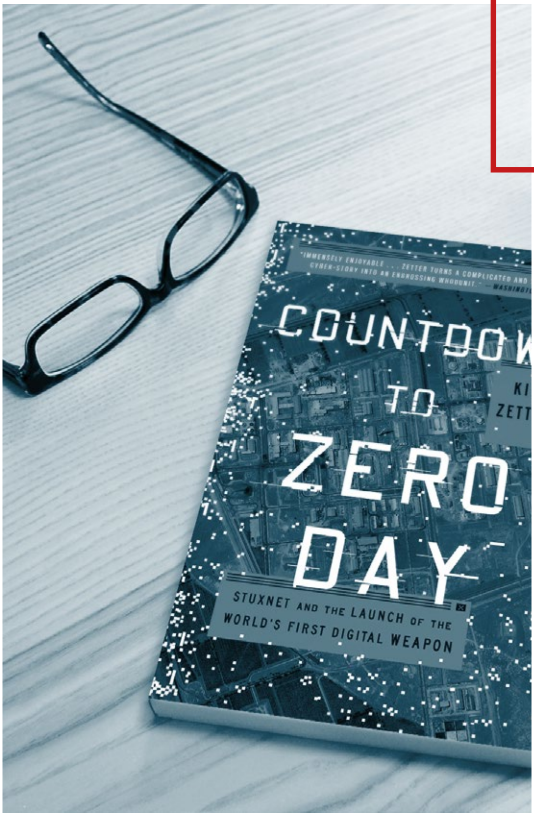
The loss of data is an ongoing challenge and impacts the heart of our work. A combination of legislative and technological developments, such as 5G and the redaction of WHOIS, will significantly inhibit the attribution and location of suspects for law enforcements and security researchers. Also, cybercriminals' continued abuse of encryption is making it more and more difficult to obtain information. In response to this challenge, Europol is cooperating with the Joint Research Centre of the Commission to further develop advanced decryption services to the EU member states..

Keeping up with developments. Cybercrime continually evolves, creating a constant challenge for both law enforcement and prosecutors in terms of acquiring and maintaining the expertise required to successfully investigate and prosecute. ■

Questions by: Barbara Sztokfisz

Interview with Kim Zetter

award-winning investigative journalist



on the book *Countdown to Zero Day: Stuxnet and the Launch of the World's First Digital Weapon*

Kim Zetter is an award-winning investigative journalist and book author who has been covering privacy, cybersecurity, national security and the hacking underground since 1999, first for PC World magazine and more recently for WIRED, where she wrote about security, cybercrime, surveillance and civil liberties for more than a decade. She has broken numerous stories over the years and has three times been voted one of the top 10 security reporters in the US by her journalism peers and security industry professionals. She's considered one of the world's experts on Stuxnet, a virus/worm used to sabotage Iran's nuclear program, and has published a highly-acclaimed book on the topic - Countdown to Zero Day: Stuxnet and the Launch of the World's First Digital Weapon. The book was translated into Polish and became available in Poland in 2018.

Welcome, Kim, and thank you for accepting this interview. As a first question, I would like to ask you to describe your book. I was reading through and I thought: Is this a documentary? Is this a historical thriller? Is this a career guide? How would you describe it?

I like the idea that it would be a thriller. It is authentic, it is nonfiction. The story of the creation of Stuxnet, and more significantly its discovery and how it was taken apart, is told like a detective story. It is about the researchers who initially discovered it, beginning in Belarus and then around the world, and about how other researchers in the US took it apart. It is in fact a story of how they figured out what it was designed to do, how it was created, but also what were the ramifications of Stuxnet. One of my goals was, first of all, to shine a light on the work that cybersecurity researchers do, which I find fascinating, and the expertise that they put into these kinds of activities to help give us more security. Stuxnet really changed their job. It politicised cybersecurity research and I wanted to address that aspect, especially for an international company like Symantec, which is where the researchers were from.

> **One of my goals was, first of all, to shine a light on the work that cybersecurity researchers do, which I find fascinating, and the expertise that they put into these kinds of activities to help give us more security.**

When you say that cybersecurity research was politicised, what do you actually mean by that?

It became obvious very quickly – within the first couple of weeks after the researchers started examining it – that Stuxnet was a nation-state attack. Given who the target was – Iran – there weren't that many nation-states that were capable of the kind of sophisticated attack this was, and that also would have the motive to attack Iran. It was down to only a handful. It became clear pretty early for them that it was probably created by the US.

Symantec is based in the US, but it is an international company. At that time, this was the first real APT (advanced persistent threat) nation-state attack. Certainly, we have had some Chinese APT attacks that targeted the US in 2010, but this was the first time that we were looking at an international company investigating an attack that had been launched by their own country. The researchers were not told to abandon the research and were able take the code apart, so they continued to reverse-engineer it. Over the period of four months, they published multiple progress reports and they told me that no one interfered, no one came to them from the government, no one came to them from management at Symantec and told them to stand down or not to publish something. I don't think that would be the case today.

Considering the place, how difficult was it to research the book and how difficult was it to get it published? Was there any official pushback, did you encounter any opposition?

No, no pushback at all and certainly not from the government. In fact, after the book was published, people really embraced it. I got a lot of gratitude from government figures who felt like the issue of cyber warfare wasn't being discussed, that it was kept classified and under wraps. They told me that having it out in a book allowed them to point to it in discussions, in classes and among military personnel.

As I said, it was quite difficult to classify exactly what your book is. I was also curious to know what your intended audience was.

I was aiming it at people who wanted to get into the cybersecurity field, but also at the general public, to let them know that this is something our government and other governments are engaging in and we need to be aware of it. And I was really aiming it at policy-makers as well, who weren't aware that this was going on and weren't aware that the techniques and the tactics were far ahead of policy-making, so we needed to catch up.

It is incredibly detailed. But for our technical audience, what do you think the most important takeaways would be?

Stuxnet was considered state-of-the-art at the time. It was discovered in 2010 and what it was designed to do was phenomenal. This was the first digital attack that leapt from the digital world into the physical world, causing physical destruction not to the computers that were infected, but to devices that these computers controlled – the Iranian centrifuges. It did it in a really ingenious way. It got onto the system and it maintained its presence for years.

The first infection was probably around late 2007, and it wasn't discovered until 2010, meaning that it remained under the radar for three years. During that time, Stuxnet would record the normal operations of the computers and the centrifuges: the speed at which they were spinning, the temperature and pressure inside. In addition, while it was sabotaging the system, it was feeding false data back to the operators so that they couldn't see on their monitoring stations what was happening to the centrifuges. Stuxnet was also designed to look for attempts to find it. If the engineers at the Natanz facility saw that there were issues with the centrifuges and couldn't figure out what was happening, of course, one of the first steps they would want to take is to look at the code on the devices and see if it had been corrupted in any way. Stuxnet was actually looking out for that, looking for any commands that were designed to read the coding on the system, and it would intercept that code going back to the monitors and scrub clean all of its malicious code, so that only disinfected code would be delivered to the engineers. And if they decided to wipe the systems clean and restart with new code, Stuxnet was watching for that as well. It would grab any new code coming in and inject its malicious code into those code blocks so that it remained active all the time.

This was the first digital attack that leapt from the digital world into the physical world, causing physical destruction not to the computers that were infected, but to devices that the computers controlled – the Iranian centrifuges.

I must say I really enjoyed how smart this was, and I think my favourite was the doppelganger DLL. I just wonder what was your favourite method or technique as you went through? What caught your imagination the most?

I think it was the way it maintained secrecy and persistence, the way that it recorded the normal operations and then fed back that information to the operators to keep them in the dark about what was happening. But I should point out that once Stuxnet was discovered, and the researchers were able to fingerprint it to find the code it was using, the encryption keys and other related things, this actually allowed them to find a whole host of other malware written by the same group of attackers.

Nation-state attackers have learned lessons from Stuxnet. For instance, you don't re-use code, because once one piece of your code is discovered, then if you have re-used it in other weapons, those are also going to be discovered quickly. When Stuxnet fell, there were about half a dozen other major pieces of malware that the US and Israel had designed that also fell subsequently afterwards. That part was really interesting to me. They invested so much time and so much money in this very expensive tool. They created an entire platform around it for spy tools. In order to make a precision weapon designed to only attack one very specific facility, the code had to be very precise. And in order to write precise code, you have to know exactly the configuration of the system that you are attacking. That must have taken a lot of intelligence. These were systems that weren't connected to the Internet, so they designed espionage tools to extract that configuration information. And all these tools were related — they used the same infrastructure, the same code for exfiltration of data. And when Stuxnet fell, all the rest of them fell as well.

Nation-state attackers have learned lessons from Stuxnet. For instance, you don't re-use code because once one piece of your code is discovered, then if you have re-used it in other weapons, those are also going to be discovered quickly.

Talking to the research community, do you think Stuxnet has helped improve the security of industrial control systems and critical infrastructure?

Yes, immensely. Prior to the discovery of Stuxnet, no one was really paying attention to industrial control systems. Researchers at Symantec had never looked at industrial control systems before.

Stuxnet was written in a unique language used by such systems, and it was a language the Symantec researchers had never seen before. For them, reverse-engineering the malware wasn't just about trying to figure out what the binary was designed to do; because it was written in a programming language that they didn't understand, even when they reverse-engineered the code, they couldn't understand the commands describing what it was doing. So, they reverse-engineered it in one stage, and then it is still a foreign language to them. They had to learn what that coding language was in order to decipher what the commands were.

Stuxnet created widespread interest in cybersecurity focused on industrial control systems. This is a niche aspect of cybersecurity, and there weren't that many people involved in it at that time, in 2010. There were maybe three or four companies that excelled in this; and now there is a whole host of companies that are focused on critical infrastructure and industrial control systems.

Stuxnet created widespread interest incybersecurity focused onindustrial control systems.

You mentioned one of the researchers said that he expected a wave of copycat attacks in the wake of discovery, but it hasn't really happened. Why, do you think?

We all thought that once Stuxnet was discovered and taken apart, it opened the way for attacks on critical infrastructure. Because it didn't just shine a light on the vulnerabilities with industrial control systems for security researchers, it also shone a light on these vulnerable systems for attackers and gave them ideas about launching similar assaults. So, everyone thought that critical infrastructure would be inundated with a lot of attacks, but they weren't. I think that is partly because these systems are pretty sophisticated. If you want to just cause a random destructive attack, it doesn't take a lot of skill, but if you want to launch a stealth attack and a precision attack like Stuxnet was, it does take immense skill and testing. One of the reasons we haven't seen other attacks like Stuxnet is that the people who have the will don't have the skill, and people who have the skill don't necessarily have the will yet.

But there should be a caveat to that: we don't know what we don't know. We see power outages all the time, and there was a series of pipelines explosions in Iran around the same time Stuxnet was attacking the centrifuges. Pipelines use the exact same industrial control systems that Stuxnet was attacking. There are always these sorts of incidents that happen around the world, and usually they are attributed to a non-cyber-related cause – not a cyberattack. But we don't know if those are the real explanations or if some of these have been caused by cyberattacks.

Actually, we did see a comparable attack to Stuxnet – the Ukraine power outage in 2015. It wasn't as sophisticated as Stuxnet, and the degree of destruction was different too. But that was the second time we saw a nation-state going after the critical infrastructure of another state in an attack that caused some physical effect and some physical damage.

Your book makes it very clear that those who put the Stuxnet attack together went to extraordinary lengths to make sure that it couldn't be traced back to them, and yet we have this attribution to the US and Israel. How did that happen?

This was interesting. One of the first things that President Obama reportedly asked after it became clear that Stuxnet had been discovered was whether it could be traced back to the US. He was told that it was absolutely impossible. It is true, from the code, it can't be traced back to the US definitively. But we don't do attribution just through code forensics. We do attribution through signals intelligence and through journalists reporting from anonymous sources. Iran didn't have the signals intelligence to be able to trace it to the US, but there were anonymous sources who told reporters that the US and Israel were responsible for it. And the US and other countries, of course, do have the ability to collect signals intelligence in order to trace and attribute attacks. Even when we see false-flag operations designed to forensically confuse investigators by introducing code that could point to another country, signals intelligence can still sometimes determine the true source of an attack. The signals intelligence seems to be the most reliable method at this point for attribution, along with reporting by journalists with anonymous sources.

Do you think there has now been a change of approach? Of my discussions with Howard Schmidt[1], he was always concerned about the boomerang effect. Unlike conventional arms, the evidence of what you did in cyberspace is not destroyed for the attackers and so it can always come straight back at you. Do you think there has been a shift in governments' approach to this?

I think there is recognition that with a digital weapon someone can reverse-engineer the code and design an attack that comes back at you. But I think that even though there is that caution, the resistance to using digital weapons, at least in the US, has dropped. I went into the book thinking that there was no way that Stuxnet was the first digital weapon the US had used. It just didn't make sense to me, because they had started doing research on these types of weapons back in the mid-90s. I was convinced this was not the first. But when I spoke with General Michael Hayden[2], he said that the legal barriers to getting something like this past the lawyers were so great that most of the time they didn't even suggest such operations. But Stuxnet was the proof of concept. It showed people who didn't know about this, it showed the government and policy-makers within the military, what the capabilities were. It proved itself. It lessened the barriers, and we have seen it with President Trump who initiated policies to increase the use of offensive operations. Reluctance is gone, and it is just a matter of legal discussions now on how to make it work.

Unsurprisingly, the book ends with a bleak note about opening the digital Pandora's box. Where does this lead us?

Stuxnet opened the door for other countries to follow suit. Basically, it gave permission to see such offensive operations as a viable option for resolving their political disputes. Of course, that also opened the way for attacks from countries that don't have the resources to conduct a traditional physical kinetic attack — countries that either don't have the military to do such attacks or don't have the ability to be stealthy. You don't need a lot of resources to mount an ordinary offensive cyberattack against critical infrastructure. You do need resources for something exactly like Stuxnet, that is precise and brimming with stealth capability, but you can hire the skillset. There are hackers who are mercenaries. Stuxnet opened a whole new vista for other actors to follow suit, and after Stuxnet, more than 20 other nations announced plans to develop capabilities to launch offensive operations.

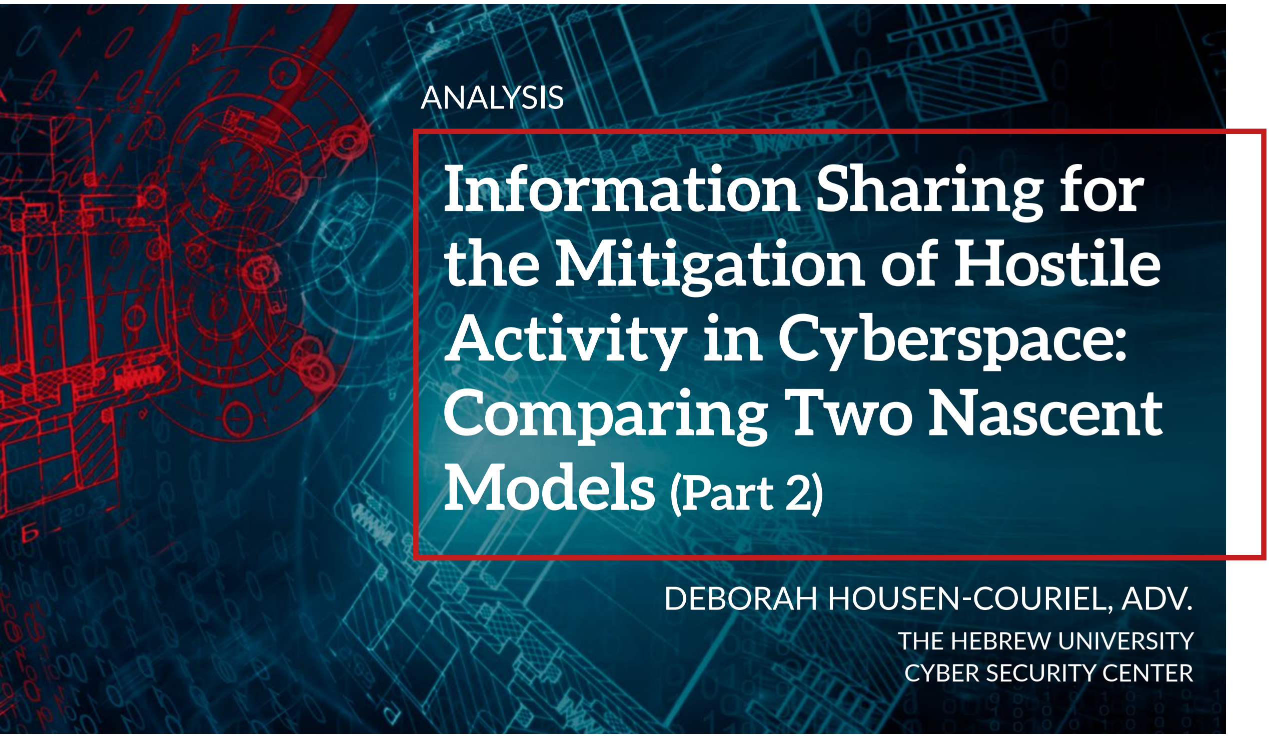
I thoroughly enjoyed this book and I recommend it to anyone who is interested in cybersecurity and in Stuxnet. Let's hope that the lessons will be learned. Thank you. ■

Interviewer: Warwick Ashford, Security Editor at Computer Weekly

This article is based on an onstage interview that took place on 8 October 2018 at the 4th European Cybersecurity Forum – CYBERSEC 2018 in Krakow, Poland. It has been edited for clarity.

[1] Howard Anthony Schmidt was cybersecurity coordinator for the Obama administration from 2009 to 2012

[2] General Michael Hayden was director of the Central Intelligence Agency from 2006 to 2009 and director of the National Security Agency from 1999 to 2005.



ANALYSIS

Information Sharing for the Mitigation of Hostile Activity in Cyberspace: Comparing Two Nascent Models (Part 2)

DEBORAH HOUSEN-COURIEL, ADV.
THE HEBREW UNIVERSITY
CYBER SECURITY CENTER

1. Recapping: Information Sharing as an Element of Cybersecurity

In the first section of this two-part article (Housen-Couriel, 2018), we argued that information sharing (IS) among private sector and governmental entities can serve as an effective tool for bolstering cybersecurity and mitigating damage caused by hostile cyber incidents. Nonetheless, in the absence of regulation mandating IS, private sector actors may be reluctant to share information voluntarily; and even when government regulation requires IS, private sector actors' participation may not be optimal. The drawbacks they currently ascribe to IS platforms include imperfect trust relationships among participants; a lack of transparency regarding the efficiency and confidentiality of the IS process; exposure to legal liability with respect to the information shared (i.e. protected personal data or intellectual property); and operational and personnel costs related to participation in IS platforms (ENISA, 2017).

In the second part of this two-part article, we briefly analyse and compare two current IS developments in light of these overarching concerns. The first is the 2016 EU Network and Information Systems Directive (NIS) that came into effect in May 2018[1]; and the second is Israel's Cyber and Finance Continuity Center (IFC3), established in January 2017 as a joint initiative of the Ministry of Finance and the Cyber Directorate (Ministry of Finance, n.d.; Ministry of Finance, 2017, September 4). NIS is a mandatory regulatory framework that applies to all EU member states and, once fully transposed, to a broad spectrum of organisational sectors in which states designate the operators of essential services (i.e. energy, transport, water supply) and to digital service providers[2].

[1] Directive 2016/1148 concerning Measures for a High Common Level of Security of Network and Information Systems Across the Union, 2016 OJ (L 194/1) [hereinafter NIS].

[2] The deadline for NIS transposition was set for May 9, 2018: as of this writing 12 of the 28 member-states have taken action (Cyprus, Czech Republic, Estonia, Finland, Germany, Italy, Malta, Netherlands, Slovakia, Slovenia, Sweden, UK). See European Commission. (2018, May 4).

Under the NIS, member states are required to exchange cybersecurity-related information on an ongoing basis; and domestic operators and providers, including private sector actors from seven diverse sectors, are required to share information through a regulatory notification regime. In contrast to the NIS model, the IFC3 is a national IS platform, specific to the financial sector, and voluntary.

In the first part of the article we examined IS as a measure that contributes to optimal jurisdictional cybersecurity, whether the jurisdiction is sectoral, national, or trans-national. In this second part, we analyse and compare the IS measures and modalities of NIS and the IFC3 as well as several issues that emerge from their comparison. The conclusion points to two key future challenges: (a) the special case of IS arising from responsible disclosure of cyber vulnerabilities; and (b) the imperative to include new stakeholders, such as individual end-users of cyber products and services, in innovative ways that maintain trusted IS relationships.

2. Comparing the EU NIS and the IFC3

The two nascent initiatives aim to bolster cybersecurity in their respective jurisdictions through IS among governmental bodies and private sector organisations[3]. They do so by promoting IS as an integral, strategic element of overall preparedness and resilience. Under both frameworks the information sharing *praxis* is currently evolving. Nevertheless, we propose that as they are increasingly implemented, each model holds insights for the functioning of its counterpart.

3. Information sharing under the EU NIS Directive

The EU has moved ahead in recent years with several key regulatory developments to increase cybersecurity, including its 2013 Cybersecurity Strategy (European Commission, 2013, February 7), the 2016 Communication on Cyber Resilience (European Commission, 2016, July 5), the GDPR[4], and upgraded authorities for the European Agency for Network and Information Security (ENISA)[5]. In the context of these developments, the NIS Directive entered into force in August 2016 with a deadline of May 9, 2018 for transposition into national laws of member states (NIS, 2016, Article 25)[6]. The directive establishes a pan-EU framework for regulatory measures and technical requirements to support IS among relevant state and private sector actors to counter cyber risks and hostile incidents, while safeguarding protected personal data and other protected data types (ETSI, 2017, p. 7).

The goal of the NIS is to achieve a high common level of network and information security among member states by requiring them to implement a basket of common measures for cooperation at two interlocking levels: (a) the multilateral EU plane; and (b) within member states' domestic jurisdictions (ETSI, 2017, pp. 5-6)[7].

[3] At present, the latter include only commercial enterprises. By way of contrast, there are information-sharing platforms that include universities, non-profit organisations and individuals as participants, such as Luxembourg's MISP – Malware Information Sharing Platform (www.misp-project.org), the UK's Threatvine (www.surevine.com/threatvine/), and Australia's Joint Cyber Security Centres (www.cert.gov.au/jcsc/jcsc-partners).

[4] Regulation (EU) 2016/679 of 27 April 2016 on the Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Movement of Such Data, and Repealing Directive 95/46/EC (General Data Protection Regulation), 2016 OJ (L 119/1).

[5] Regulation (EU) 526/2013 of 21 May 2013 concerning the European Union Agency for Network and Information Security, 2013 OJ (L 165/ 41).

[6] See the status of transposition by member states in the references at supra note 2.

[7] These measures include: adoption of a *national information security strategy*; establishment of a *Cooperation Group* to coordinate implementation; establishment of *national competent authorities* and *single points of contact*; the obligation of states to designate the abovementioned "operators of essential services" and "digital service providers"; states' obligation to enforce incident notification and other requirements; establishment of a network of CSIRTs; implementation of cyber risk management practices and controls; and international cooperation promoting a global approach to standards and information exchange.

IS constitutes a key element at both the EU and national levels and is established to support the overarching NIS goals for cyber incident management and response, as well as building trust among stakeholders. The key paradigm is that of "structured information sharing" regarding incidents and risks, implemented at both the EU and national levels (ETSI, 2017, pp. 6, 11-12). NIS establishes two types of IS through notification: compulsory and voluntary.

3.1 Compulsory notification requirements

The first IS context is the compulsory notification requirement for cyber incidents having a "significant impact" that devolves upon designated operators of essential services, and a similar "substantial effect" for digital service providers[8]. Articles 14 and 16 of the NIS Directive set out this requirement in similar language, as follows:

> Member States shall ensure that operators of essential services notify, without undue delay, the competent authority or the CSIRT of incidents having a significant impact ["substantial impact", for digital service providers] on the continuity of the essential services they provide [or on the provision of a service they offer]. Notifications shall include information enabling the competent authority or the CSIRT to determine any cross-border impact of the incident. Notification shall not make the notifying party subject to increased liability.

This provision is applied in the first instance within a national jurisdiction, and thus determines the significance or substance of the impact of a given incident subject to the common NIS criteria provided in Articles 14(4) and 16(4). The national competent authority or CSIRT then determines whether the information should be shared with other EU member states. At this second level of trans-national IS among EU members, explicit substantive constraints on IS apply, as follows:

- The information exchanged is limited to data which is *relevant and proportionate* to the purpose of the IS (NIS, 2016, Article 1(5); 12(3)(b) and (c); Recitals 40-41);
- The *confidentiality* of information is preserved, as are the *security and commercial interests* of operators and providers (NIS, 2016, Article 1(5); 12(3)(b) and (c); Recitals 40-41);
- *GDPR safeguards apply* with respect to IS of personal data (NIS, 2016, Article 2);
- IS takes place without prejudice to *essential national security interests* under Article 346 of the TFEU (NIS, 2016, Article 1(5));
- Trans-national IS carries forward the *exemption from increased liability* for the notifying party specified in Articles 14 and 16.

3.2 Voluntary IS

The second context is *IS through voluntary notification*[9]. This mode of information sharing is established under NIS Article 20 for "any reasonably identifiable circumstance or event having a potential adverse effect on the security of networks and information systems..." (ETSI, 2017; NIS, 2016), as follows:

> [E]ntities which have not been identified as operators of essential services and are not digital service providers may notify, on a voluntary basis, incidents having a significant impact on the continuity of the services which they provide.

The same explicit legal constraints apply to voluntary notification as have been specified above, with respect to compulsory notification requirements (NIS, 2016, Article 20(1)). Thus, some of the normative challenges for private sector participants for voluntary IS that were noted in section 2 above have been addressed explicitly within NIS, with

[8] See the criteria for determining "significant impact" in NIS Article 14(4) and "substantial impact" in NIS Article 16(4); and Annexes II and III and Recitals 9-20 on criteria for member states' to designate their operators of essential services and digital service providers.

[9] There is a certain overlap of the two contexts, for example in NIS Article 14(5). For the reporting procedures on the part of operators and service providers, see Articles 6,14-17. In this context the NIS adopts the terminology of "information exchange" rather than IS, to which it refers exclusively in the context of preserving trusted legacy IS mechanisms (NIS Article 5 and Recitals 35 and 59).

safeguards provided by commercial confidentiality and personal data protection specifically incorporated. Moreover, entities that opt for voluntary notification do not incur any of the additional responsibilities that may follow from obligatory notification, such as being required to notify the public regarding a specific cyber incident[10].

Finally, the modes of implementation of IS in both the obligatory and voluntary contexts are described in NIS Articles 8-13. The national competent authorities are charged with this responsibility through their participation in the Cooperation Group (NIS, 2016, Article 11); and the requirement that they designate a national CSIRT to participate in the pan-EU CSIRT network[11]. The CSIRTs themselves are charged with operative IS which is, for the present, voluntary for private sector stakeholders unless their participation is compelled by other, non-NIS regulation[12]. The relevant NIS Annex, entitled "Requirements and Tasks of CSIRTs", stipulates their monitoring of risks and incidents; the provision of alerts and other operative indicators to stakeholders; as well as support for incident response.

Although the NIS has only recently come into force, the mandated IS platforms are already in place and operational: and the directive is likely to incentivise and optimise participation in these existing IS platforms.

In summarising this brief look at IS under the NIS, we emphasise the explicit substantive safeguards that obtain at both the national and trans-national levels: the confidentiality of shared information is preserved, as are the security and commercial interests of sharing entities and their exemption from any increased liability. Moreover, at the practical level, the inclusion of CSIRTs as the operational infrastructure of this directive builds existing IS capabilities into the new legal framework: all EU member states currently have CSIRTs (or similar CERTs) in place (ENISA, n.d., p. 25). The NIS promotes a formalisation of their mandate and operations as part of the pan-EU IS infrastructure. Moreover, ENISA has initiated a CSIRT assessment program in the NIS framework, including an EU-wide accreditation scheme (ENISA, 2016, p. 25). Thus, although the NIS has only recently come into force, the mandated IS platforms are already in place and operational: and the directive is likely to incentivise and optimise participation in these existing IS platforms (Katulić, 2018).

4. Information sharing at Israel's IFC3

4.1 Regulatory background: an absence of obligatory IS

Israel's regulatory engagement with various aspects of cybersecurity at the national level began relatively early in the mid-1990s with several legal initiatives, including the Computers Law of 1995, the Law for Regulating Security in Public Bodies of 1998 and Resolution B/84 of the Ministerial Security Committee Decision of 2002 (Tabansky and Ben Israel, 2015). A major focus on a national strategy, institutional preparedness and workforce development began with the August 2011 government resolution No. 3611 entitled *Advancing National Cyberspace Capabilities* and establishing the National Cyber Bureau (NCB) as the lead governmental agency for cybersecurity policy coordination[13]. Two subsequent government resolutions followed in 2015, *Advancing National Regulation and Governmental Leadership in Cyber Security* (No. 2443) and *Advancing the National Preparedness for Cybersecurity* (No. 2444) to promote specific elements of national

[10] "Voluntary notification shall not result in the imposition upon the notifying entity of any obligations to which it would not have been subject had it not given that notification", NIS Article 20(1).

[11] NIS Article 12. The national CSIRT must be provided with adequate support for fulfilment of its tasks (NIS Article 9).

[12] See, for instance, NIS Article 1(7).

[13] Among the goals of this initial government resolution were "to advance coordination and cooperation" among government bodies and other sectors, to produce an annual document on cyber threat vectors, and to publish "warnings and information for the public regarding cyber threats", yet these aims stop short of full information-sharing measures (Government Resolution 3611, 2011, August 7).

cybersecurity, including the establishment of a national CERT and the first references to IS measures (Housen-Couriel, 2017). Resolution 2443, which addresses internal government measures, mandates development of "processes for information sharing inside the government, including reporting to the National CERT" (Government of Israel, 2015a, Article 3c of Addendum E). The complementary Resolution 2444, which addresses the Israeli cyber ecosystem as a whole, charges the National Cyber Bureau with establishing, together with the National Cyber Authority:

> A national technological and organisational infrastructure for early warning, analysis, alert and sharing of information, in order to expose and identify cyberattacks on the State of Israel. This will be in accordance with the recommendations to be formulated […] with regard to aspects related to the establishment of this infrastructure […] *including the scope of information to be collected, the format of its use, and how it is to be protected and shared*. (Government of Israel, 2015b, Article 5)[14].

Thus, Resolution 2444 explicitly mandates the establishment of a national IS mechanism, although it refrains from imposing a regulatory requirement on organisations for information sharing or notification. Indeed, at present there are no compulsory IS measures for cybersecurity in Israel that are imposed on private sector entities by national legislation[15]. Some notifications are required by certain entities that are classified as critical infrastructure, although such notifications are largely not transparent to the public and are not categorised as IS for present purposes (Haber and Zarsky, 2017)[16].

4.2 Information-sharing developments in the financial sector

Nonetheless, interesting developments with respect to sectoral information sharing are evident in two promulgated directives that relate to IS in the banking and financial services sectors. The first is the Bank of Israel's March 2015 Cyber Defense Management Directive No. 361, which provides that "[t]he banking corporation shall share information that may help other banking corporations in handling cyber threats" (Bank of Israel, 2015), *via* modalities which will be determined by future directives that have yet to be published at the time of this writing. The second is the Supervisor of Capital Markets' August 2016 Directive on the Management of Cyber Risks, which prescribes an obligation on financial sector organisations only to *consider* sharing information with Israel's national CERT that may be relevant to cyber risk or to operative situations (Supervisor of Capital Markets, 2016, Article 5(a)(1)(b))[17]. A third relevant regulatory development for information sharing is the March 2017 Public Statement issued by Israel's Antitrust Authority, providing clarification on IS for cybersecurity for all Israeli organisations and exempting such IS from antitrust sanctions when certain conditions are fulfilled (Antitrust Commissioner, 2017).

Thus, despite this lack of any formal, compulsory regulatory requirements prescribing the parameters and modalities of IS for Israel's financial sectors, sectoral interest in a viable IS platform has been awakened and has motivated a high level of participation in voluntary IS through IFC3. We propose that this interest may also be motivated

[14] See also Article 2 on the National Cyber Authority's responsibilities with respect to fostering cooperation among various sectors.

[15] Such compulsory measures have been included in a proposed bill for Israel's national cybersecurity law of June 2018 (Government Bill on Cybersecurity and the National Cyber Directorate 2018 (in Hebrew), at 40 and Articles 16, 17, 65 and 66). Moreover, in the explanatory notes to the Bill there is an explicit reference to the NIS provisions for IS (at 15).

[16] Critical infrastructure systems are subject to IS requirements that are largely non-transparent. There are also regulatory requirements to notify the data privacy regulator about certain incidents under Article 11 of the Privacy Protection Regulations (Data Security) 5777-2017, and the Israel Stock Exchange about risks and incidents that may have a significant impact on a company or its share price (Article 36, Securities Regulations (Periodic and Immediate Reports), 5730-1970).

[17] Reporting to the Supervisor of Capital Markets is required only for two types of "significant" incidents (Article 5(a)(11)). *See also* the support given by the Capital Markets Supervisor for the contribution of IS to cybersecurity following an audit of cybersecurity in this sector (Supervisor of Capital Markets, *Results of a Cyber Audit*, 8.7.2018. (in Hebrew)).

by the need to comply with other required elements of the Bank of Israel and Capital Markets directives, IS having become increasingly critical to effective organisational compliance to these other stipulations.

4.3 The establishment and operation of IFC3

In January 2017 the Israeli government established the Cyber and Finance Continuity Center (IFC3) under the joint aegis of the Ministry of Finance's Cyber, Emergency and Security Division and the Cyber Directorate (Weis, 2017, September 17). These two government regulators currently operate IFC3, which is located on the premises of Israel's national CERT in the southern city of Beersheba. At present, around forty organisations voluntarily participate in the IS platform on the basis of CERT-IL's declaration of operating principles and a non-disclosure agreement to which each organisation has adhered (National Cyber Authority, n.d.). They include all major banks, credit card firms, financial services firms, financial trade associations, and financial utilities and insurance companies (Ministry of Finance, 2017, September 4).

The IFC3 divides its IS capabilities into four areas: general cybersecurity, cyber fraud, business continuity, and innovation (Weis and Shtokhamer, 2017, June 25; Shtokhamer, 2018, June 19). In its first six months of activity, IFC3 prepared and distributed to its members 120 alerts based on shared information; dealt with 45 sectoral hostile cyber events, including the WannaCry ransomware attack in May 2017; and conducted a cyber exercise together with similar centres outside Israel (Weis and Shtokhamer, 2017, June 25).

The response of IFC3 to the WannaCry events, in particular, exemplified the importance of sector-wide IS and response coordination. FC3 had shared information to its participants on the Shadow Brokers group April 2017 leak of NSA vulnerabilities that were eventually used in the WannaCry attack a month later. The situation was monitored on an ongoing basis until the beginning of the attack on May 12, when members shared information through the automated system used by the platform for real-time indicators, including operative cyber-defence indicators, and participated in a WannaCry simulation to examine their own vulnerabilities during unfolding events.

The response of IFC3 to the WannaCry events, in particular, exemplified the importance of sector-wide IS and response coordination.

The outcome of a relatively low rate of WannaCry impact on the Israeli financial sector cannot be attributed solely to the IFC3 platform's IS, yet participants have stated that the IS measures were effective in real-time and it may have been a contributing factor (Weis and Shtokhamer, 2017, June 25). The high level of *de facto* participation in the WannaCry simulation and the IS around actual events is attributed to the trusted environment that has demonstrated its reliability and value to users over a relatively short period of time (Weis, 2017, September 17).

5. Analysis and insights

In comparing the EU's NIS-mandated platform for IS and Israel's IFC3 it is clear that both models use IS as part of a broader jurisdictional and policy approach to cybersecurity. Their comparison and analysis below address three aspects:

- **Formal regulatory requirements v. voluntary participation**

The EU has taken a more formally regulated approach that provides for relatively complex institutional interaction (Cooperation Council, 28 national competent authorities, points of contact, and a network of CSIRTs). It also requires national legislation for its full implementation. In contrast, Israel has yet to regulate mandatory IS at the level of national legislation: government decisions, sectoral directives, and some second-tier regulation, including CERT-IL's declaration of operating principles, constitute its current provisions in this matter.

- **Scaling up: intra-sectoral, inter-sectoral and inter-jurisdictional IS**

It may be argued that the IFC3 model more readily bolsters trust relationships because of the smaller number of participants than those in the national CERTs and pan-EU IS mechanisms. The sectoral model provides sharers with a common professional language, understanding of risk and regulatory constraints; and professional networks and connections may ease voluntary participation in an IS platform[18]. NIS may be able to leverage this IFC3 advantage by eventually "sectoralising" its CSIRT network; on the other hand, the IFC3 stands to gain by scaling up to collaborate across other Israeli sectoral lines[19]. In accordance with the network advantages that can be gained by inter-jurisdictional IS, both models incorporate mechanisms for such sharing, although they are beyond the scope of the present analysis (NIS, 2016, Article 13; National Cyber Authority, n.d.).

- **Substantive constraints on IS**

NIS provides a key element missing from the Israeli model: explicit substantive constraints with respect to the relevance and proportionality of IS, confidentiality and data protection, and the limitation of liability for sharers. These important constraints are likely to contribute to the long-term credibility of the NIS platform, as sharers can better understand the parameters of their participation, calibrate expectations, and have recourse should such issues arise. The IFC3 currently relies upon two informal documents for elaboration of these constraints, the Antitrust Authority's Public Statement of March 2017 and the *CERT Operating Principles*. Although it may at present be able to resolve these considerations "in-house", by leveraging the trust relationships that have developed through utilisation of the platform and its reliability, it is critical for Israel's evolving IS platforms – IFC3 and others – that overarching principles and legal constraints be in place transparently and at the legislative level for this evolution to proceed in an optimal manner[20].

Incomparing the EU's NIS-mandated platform for IS and Israel's IFC3 it is clear that both models use IS as part of abroader jurisdictional and policy approach to cybersecurity.

6. Conclusions and next challenges

As discussed in the first part of this article, differing approaches to the regulation of IS platforms have an impact on their effectiveness. In particular, the ways in which government actors and private sector entities interact for IS and whether interactions are obligatory or voluntary are likely to drive levels of trust that contribute to the optimisation of IS platforms for private sector institutions and to incentivise their participation.

We noted at the outset of this article that both NIS and IFC3 are in the early stages of their development and that additional *praxis* is necessary to draw firm conclusions about improving these IS models. In conclusion, we argue that practical experience not only needs to be garnered, but that it is critical to share the benefits and drawbacks of these IS platforms with a broader community of IS practitioners, regulators, and academics. Confidentiality is core to effective and reliable information sharing; yet to the extent that models, measures, and effective guidelines are, in their turn, shared – best practices for IS will emerge and have the potential to enhance cybersecurity across jurisdictions. Such best practices include automated protocols and tools for IS, a sharer option for anonymity with respect to other sharers, a high level of security and resilience for platforms, and inter-jurisdictional scaling up.

[18] *See* an alternative view in Siboni and Klein (2016).

[19] This may already be occurring within CERT-IL, although there is no mention of it in the *CERT Operating Principles*. *See* National Cyber Authority (n.d.). CERT Operating Principles, definition of "Cooperating entities".

[20] The proposed government cybersecurity bill does address this issue (*supra* note 15).

Practical experience not only needs to be garnered, but that it is critical to share the benefits and drawbacks of these IS platforms with a broader community of IS practitioners, regulators, and academics.

Significant challenges lie ahead for IS to ensure that the information shared is consistently relevant, timely, and sufficiently detailed to bring real added value to sharers in the IS process – be they government or private sector actors. Moreover, as our understanding of hostile activity in cyberspace and its indicators expands, IS measures and capabilities will need to develop in tandem.

We conclude by noting two future challenges for IS platforms, as they become increasingly critical to cybersecurity. The first is the development of needed levels of their confidentiality and robustness, so that they may be leveraged for the responsible disclosure of vulnerabilities through IS (The White House, 2017; National Cyber Security Center, 2013; Herpig, 2018). Secondly, new measures are needed for the inclusion of stakeholders that bring new types of data and diverse perspectives to the IS platform, such as individual end-users of cyber products and services, while ensuring that trusted relationships among sharers and the added value of IS for all of them are maintained. ■

About the author:

Deborah Housen-Couriel, Adv.

Deborah Housen-Couriel's Tel Aviv-based law practice advises global and Israeli clients on strategies for regulatory planning and compliance in the areas of cybersecurity law and regulation. She teaches courses on cyber law at Hebrew University and at the Herzliya IDC and is a lead researcher at several Israeli universities. Deborah was a member of the Group of Experts that drafted Tallinn Manual 2.0; and currently serves as a Core Expert for the MILAMOS project and as Chair of a Working Group at the Global Forum on Cyber Expertise.

References

Antitrust Commissioner. (2017). Public Statement 3/17: *Information Sharing for Coping with Cyber Threats* (in Hebrew).

Bank of Israel. (2015). Directive 361, Cyber Defense Management. Art. 65 and 66.

Computers Law. (1995). Retrieved from: http://law.co.il/media/computer-law/computers_law_nevo.pdf (in Hebrew).

ENISA. (2016). Challenges for National CSIRTs in Europe 2016: Study on CSIRT Maturity.

ENISA. (2017). *Exploring the opportunities and limitations of current Threat Intelligence Platforms*. Retrieved from: https://www.enisa.europa.eu/publications/exploring-the-opportunities-and-limitations-of-current-threat-intelligence-platforms.

ENISA. (n.d.). CSIRTs by Country. Retrieved from: https://www.enisa.europa.eu/topics/csirts-in-europe/csirt-inventory/certs-by-country-interactive-map.

ETSI. (2017). *Cyber: Implementation of the NIS Directive.* (DTR/CYBER-0021). p. 7. Retrieved from: https://www.etsi.org/deliver/etsi_tr/103400_103499/103456/01.01.01_60/tr_103456v010101p.pdf.

European Commission. (2013, February 7). Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace, JOIN 2013 final.

European Commission. (2016, July 5). Communication on Strengthening Europe's Cyber Resilience System and Fostering a Competitive and Innovative Cybersecurity Industry, COM/2016/0410 final.

European Commission. (2018, May 4). State-of-play of the transposition of the NIS Directive. Retrieved from: https://ec.europa.eu/digital-single-market/en/state-play-transposition-nis-directive.

Government of Israel. (2011, August 7). Resolution 3611 (in Hebrew).

Government of Israel. (2015a). Resolution 2443 (in Hebrew).

Government of Israel. (2015b). Resolution 2444 (in Hebrew).

Government of Israel. (2018). Bill on Cybersecurity and the National Cyber Directorate (in Hebrew).

Haber, E. and Zarsky, T. (2017). Cybersecurity for Infrastructure: A Critical Analysis, *Florida State University Law Review*, 44(2).

Herpig, S. (2018). *Governmental Vulnerability Assessment and Management*. *Stiftung Neue Verantwortung*. Retrieved from: https://www.stiftung-nv.de/sites/default/files/vulnerability_management.pdf.

Housen-Couriel, D. (2017). National Cyber Security Organization: Israel. *CCDCOE*.

Housen-Couriel, D. (2018). Information Sharing for the Mitigation of Hostile Activity in Cyberspace: Comparing two nascent models (Part 1). *European Cybersecurity Journal*, 4(3). pp. 44-50.

Katulić, T. (2018). Transposition of EU Network and Information Security Directive into National Law. *41st International Convention on Information and Communication Technology, Electronics and Microelectronics (MIPRO)*. p.1331. Retrieved from: http://docs.mipro-proceedings.com/iss/iss_03_4720.pdf

Law for Regulating Security in Public Bodies. (1998). Retrieved from: https://docs.google.com/viewer?url=http%3A%2F%2Fmain.knesset.gov.il%2FActivity%2Fcommittees%2FForeignAffairs%2FLegislationDocs%2Fsec7-2.doc (in Hebrew).

Ministerial Security Committee. (2002, December 11). Decision B/84.

Ministry of Finance. (2017, September 4). *Finance Cyber and Continuity Centre (FC3)*. Retrieved from: https://docs.google.com/viewer?url=http%3A%2F%2Fwww.export.gov.il%2Ffiles%2Fcyber%2FFC3.PDF%3Fredirect%3Dno.

Ministry of Finance. (n.d.). Cyber and Finance Continuity Center. Retrieved from: https://mof.gov.il/en/About/Units/CyberEmergenciesSafetyDraft/Pages/CyberCenterAndFinancialContinuity.aspx.

National Cyber Authority. (n.d.). CERT Operating Principles (in Hebrew).

National Cyber Security Centre. (2013). Responsible Disclosure Guideline. Retrieved from: https://www.ncsc.nl/english/current-topics/news/responsible-disclosure-guideline.html.

Robinson, N. and Disley, E. (2010). Incentives and Challenges for Information Sharing in the Context of Network and Information Security. *ENISA*.

Shtokhamer, L. (2018). *CERT Operation: Financial Case Study* (presentation).

Siboni, G. and Klein, H. (2016). Information-Sharing Challenges in an Intra-Sectorial Environment. *Military and Strategic Affairs*, 8(1), pp. 41-58.

Supervisor of Capital Markets. (2016). Circular on Management of Cyber Risk.

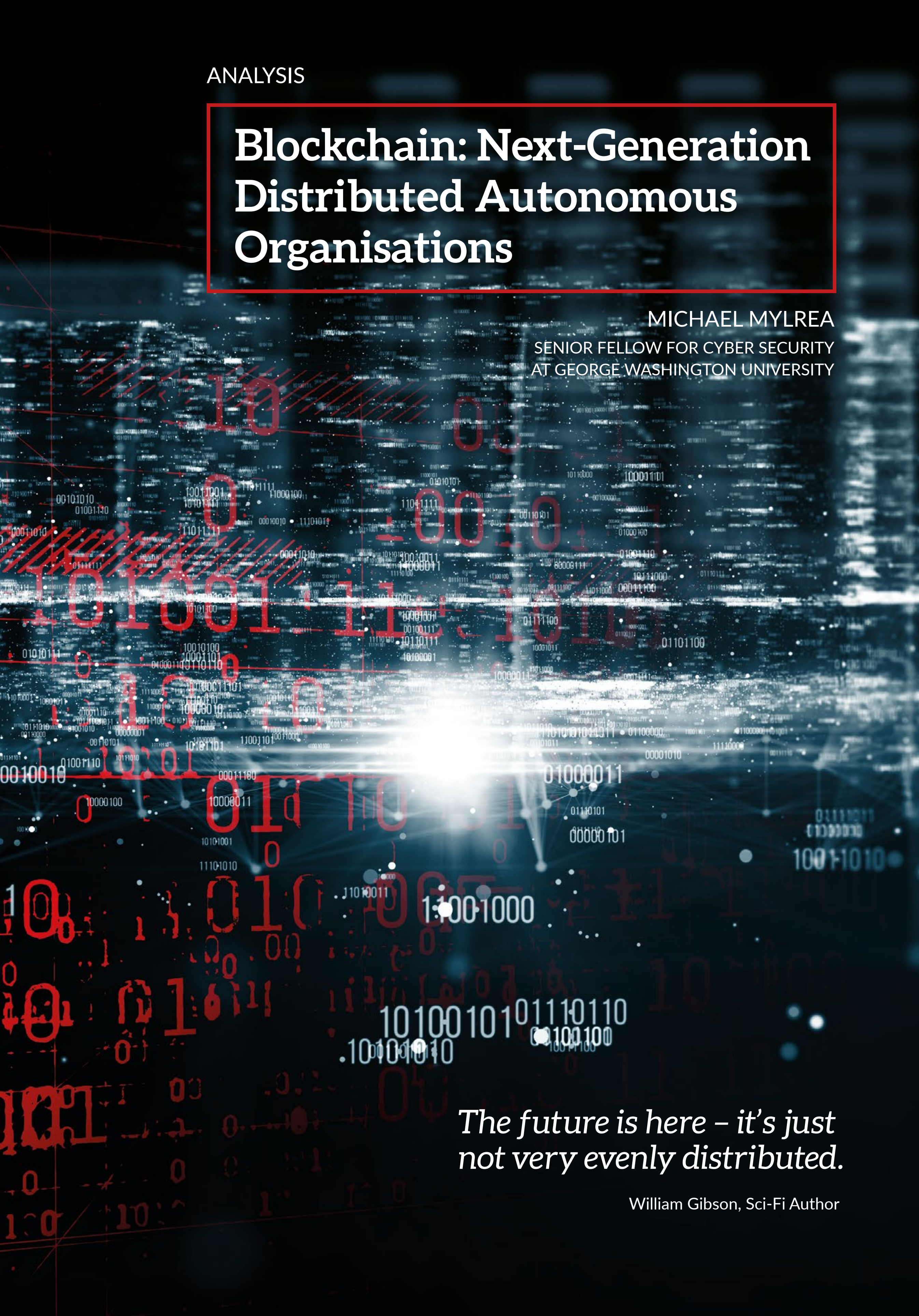
Supervisor of Capital Markets. (2018). Results of a Cyber Audit (in Hebrew).

Tabansky, L. and Ben Israel, I. (2015). *Cybersecurity in Israel*. Springer. pp. 31-34.

Weis, M. (2017, September 17). Presentation at the National Fintech Cyber Ecosystem Round Table (notes on file with author).

Weis, M. and Shtokhamer, L. (2017, June 25). *The Cyber and Finance Continuity Center* (presentation, in Hebrew).

The White House. (2017). Vulnerabilities Equities Policy and Process for the United States Government.



ANALYSIS

Blockchain: Next-Generation Distributed Autonomous Organisations

MICHAEL MYLREA
SENIOR FELLOW FOR CYBER SECURITY
AT GEORGE WASHINGTON UNIVERSITY

The future is here – it's just not very evenly distributed.

William Gibson, Sci-Fi Author

Introduction

While still at a nascent stage of adoption, blockchain technology may give impetus to the fourth industrial revolution, transforming modern infrastructures from decentralized to more distributed, resilient and intelligent. Today, most critical infrastructures, from transportation to energy, defence to financial institutions, do not collect, aggregate and exchange data in a secure way that is interoperable, smart and intelligent. A paradigm shift is needed for our smart cities infrastructures to become more intelligent, decentralized and distributed. Blockchain technology may present a disruptive solution to give impetus to this change through an atomically verifiable cryptographic signature that provides data provenance and attribution to help increase the trustworthiness and integrity for prodigious data sets that are being exchanged.

Today, smart cities increasingly weave together cyber and physical, information and operational technology, software, and hardware, with ubiquitous sensors that exchange prodigious data sets. Securing these internet-of-things (IoT) environments and the data being exchanged is not a trivial task, especially when organisations increasingly rely on a vulnerable global supply chain. A recent report by the cybersecurity firm Crowd Strike suggests that supply chain cyberattacks hit about two thirds of companies surveyed, with an average cost of $1.1 million (Daniel, 2018).

Blockchain Cybersecurity Opportunity

Blockchain technology's distributed form complements the increasingly distributed security function and requirements of global supply chains. Modern cities and their increasingly networked infrastructures have an array of vulnerable IoT. Security of these systems and networks could be significantly increased with a blockchain ledger of things for asset management and machine state integrity. Blockchain helps fill that gap securely via a digital ledger and cryptographic hash that signs the who, what, when and where of the data in a block that becomes a widely witnessed, auditable and inherently immutable event. This presents a number of potential opportunities to increase the cybersecurity of critical systems supply chains which are increasingly distributed, data driven, global and vulnerable. Blockchain also facilitates the auditability of IoT environments that have been developed through a global supply chain. This can help fill an important gap found in modern organizations, which often don't have an inventory or risk registry of their critical cyber assets, where they were developed, shipped, installed and when they were last patched. Malicious hackers continue to exploit these knowledge gaps to compromise critical systems (Mylrea, 2017). Blockchain can also increase visibility and monitoring of the machine state integrity of field devices and other embedded systems. IoT in critical infrastructures is often times not monitored, patched or securely configured, making it very challenging to identify, detect and protect against malicious cyber behavior (Mylrea, 2018a).

Blockchain provides an innovative trust anchor that can help transform decentralized cities and organizations to make them more distributed, autonomous and secure. In the process, blockchain may also disrupt various industry verticals, creating new services, markets and more distributed autonomous organizations. Blockchain's trust anchor can help disintermediate the many unnecessary third-party brokers involved in exchanges of value. A more egalitarian economy could potentially emerge as producers and consumers regain value from across the supply chain. More control over transactions would occur as consumers become prosumers. Some related use cases that are being explored, include blockchain solutions that enable owners of distributed energy resources to sell energy to their neighbours using blockchain smart contracts that execute autonomously when the agreed terms and conditions are met (Mylrea, 2018b).

Blockchain provides an innovative trust anchor that can help transform decentralised cities and organisations to make them more distributed, autonomous, and secure.

Smart Contracts

Blockchain smart contracts allow for the execution of digital code which results in various transactions within defined perimeters. These executions of complex transactions take place over the blockchain and are recorded over the distributed ledger. Smart contracts could also help automate supply chain security through dynamic patch management alerts and updates, roles-based access controls and baselining and monitoring machine state integrity. Once a smart contract is initialized on the blockchain, it gets an address associated with it. That address can be used to interact with the smart contract. That smart contract is present in the form of bytecode on the blockchain. Blockchain provides an atomically verifiable cryptographic signed distributed ledger, which provides a unique way of distributing trust. Instead of storing supply chain data such as inventory of critical hardware or the time of patch for critical software, critical supply chain data is stored in the distributed escrow of the blockchain, which maintains time stamped data blocks that cannot be modified retroactively, which increases the trustworthiness and integrity of the data. Several proof of authority blockchain technologies enable secure communications from operational technology protocols and industrial control systems by including an advanced cryptographic signature that assigns the time of signing and data signer as well as authentication to a data asset.

Security Features

Blockchain has several benefits that could improve cybersecurity, especially supply chain and security and identify management. Some of these benefits include:

1. Increased transparency and auditability of the system throughout the manufacturing, shipping, deployment and maintenance and retirement life cycle;
2. Immutable archived records about the firmware, hardware, and software components of the system including the past and current patch management information;
3. Expedites and enhances inter-vendor cooperative system development through increased visibility and accessibility of supply chain data;
4. Improved security of the supply chain process through increased trustworthiness and integrity of data through blockchain consensus mechanism which reduces reliance and can even replace need for intermediary trust mechanisms and brokers that are susceptible to manipulation and compromise.
5. The principle of component traceability throughout the system lifecycle to incorporate efficient systems engineering processes;
6. Improved reliability through transparency and information sharing.

There are a number of operational, technical, and policy barriers that need to be overcome to realise these valuable cybersecurity benefits.

Blockchain Barriers to Change

There is a lot of buzz around blockchain because its value proposition is exciting and potentially disruptive. However, a number of barriers remain for its full potential to be realised.

For one, blockchain means different things to different people. For this paper blockchain is defined as a distributed database or digital ledger that records transactions of value using a cryptographic signature that is inherently resistant to modification (Tapscott & Tapscott, 2016). Blockchain is a distributed database that maintains a continuously growing list of records, called blocks, secured from tampering and revision. Each block contains a timestamp and a link to a previous block. Blockchain-based smart contracts can be executed without human interaction (Franco, 2014) and the data is highly resistant to modification as the data in a block cannot be altered retroactively. Blockchain smart contracts are defined as technologies or applications that exchange value without intermediaries acting as arbiters of money and information (Tapscott & Tapscott, 2016). With those fundamentals defined, blockchains can be classified as permissioned and permissionless.

Further, there are several types of consensus mechanisms such as proof of work (PoW), proof of authority (PoA), proof of control, stake, burn, etc. (POA Network, 2017).

Blockchain technology is at a nascent stage. Evolving blockchain definitions create a number of challenges from a policy perspective. Different interpretations create misunderstanding and pose challenges for policy-makers to fill large gaps in blockchain governance, regulation, and standards. It is noted that the 'rapidly shifting, contested vocabulary poses for regulators seeking to understand, govern, and potentially use blockchain technology, and offer suggestions for how to fight through the haze of unclear language' (Walch, 2017, p. 713). One of the general misconceptions around blockchain definitions is caused by the assumption that blockchain equals Bitcoin. While blockchains include cryptocurrencies and transactions recorded publicly, private or permissioned blockchains oftentimes do not include an exchange of value and do not record anything publicly. Yet, Google defines blockchain as 'a digital ledger in which transactions made in Bitcoin or another cryptocurrency are recorded chronologically and publicly'. Similarly, Investopedia's definition associates blockchain with decentralised ledgers of cryptocurrencies: 'A blockchain is a digitized, decentralized, public ledger of all cryptocurrency transactions' (Walch, 2017).

Blockchain technology is at a nascent stage. Evolving blockchain definitions create a number of challenges from a policy perspective. Different interpretations create misunderstanding and pose challenges for policy-makers to fill large gaps in blockchain governance, regulation, and standards.

Some blockchain proponents thought the distributed ledger technologies would usher in a panacea overnight. As initial projects failed for a myriad of reasons that ranged from conflating blockchain with Bitcoin to applying blockchain to the wrong problem set, disillusionment set in. Real-world use cases are needed to highlight where blockchain has significantly improved the state of the art, cut costs, and increased security as compared to other innovative solutions from virtualisation to quantum key exchange to software-defined networking to machine learning. Real-world demos at scale can help validate and verify blockchain's application to various security challenges and optimise complex systems. Another barrier to mass blockchain adoption involves a change in functional and operational requirements and technology stack needed to incorporate the blockchain technology into an organisation.

Real-world use cases are needed to highlight where blockchain has significantly improved the state of the art, cut costs, and increased security as compared to other innovative solutions from virtualisation to quantum key exchange to software-defined networking to machine learning.

Take for example a use case that involves implementing blockchain to facilitate supply chain security. Challenges include, but are not limited to:

1. Multiple vendors are involved in product and systems development. Vendors have different levels of resources, unique constraints, and other considerations to keep in mind;
2. Vendors might be using different blockchain technologies that are not interoperable with each other or with the data being tracked. An intermediate node between different blockchains and databases can facilitate functionality in a single overall common blockchain;
3. Ability to onboard business ecosystems in terms of both functional and non-functional requirements. Moreover, reliable access to good data sets is needed. Otherwise the blockchain is providing a ledger and increased immutability with something that would be better off changed.

Additional challenges remain to give impetus to blockchain-enabled distributed autonomous organisations. Modern infrastructures need to be more interoperable and networked. Blockchain will not solve that problem alone as 90% of infrastructures are not interconnected and communicating data. Once connected, however, blockchain can take the internet of vulnerable things, and help provide a secure ledger of things for improved identity management and supply security for IoT. Another major challenge is workforce development and training. AI and blockchain may disintermediate and disrupt operations, expeditiously retiring some jobs, but if previous cycles of tech innovations are any indication, more jobs are going to be created than lost. That requires a massive investment in training the next generation on the following skill sets: secure code, parallel computing, machine learning, sociology, psychology and other cognitive behavioural studies, as these changes will transform how we interact with each other, as well as man and machine. Other limitations remain. Blockchain platforms lack the ease of use and functionality that the browser provided for the internet. In addition, blockchain solutions also lack scalability, interoperability, and universality to exchange value en masse.

Next Generation Permissioned Blockchain Solutions

Blockchain R&D continues to innovate and overcome a number of these challenges. While improvements in parallel computing have reduced transaction times and energy intensity of some of proof of work blockchain solutions, most industry grade solutions are focused on next generation permissioned blockchain solutions – like the patent pending Chios – help increase control, security and stability over proof of work solutions. Developers of Chios were able to solve 10 challenges found in a number blockchain solutions and developed a technology that is:

- Decentralized and fine-grained access control (strongest security model)
- Beyond blockchain: Publish/subscribe functionality
- Enforces causal order ("first come, first served")
- Governance: Two decentralized mechanisms for data governance
- NIST compliant; GDPR compliant
- Supports on-chain and off-chain smart contracts
- Provides easy to use application program interface
- Improves scalability in terms of services it can handle
- Improves efficiency compared to a number of other popular blockchain solutions
- Provides a stable version for arbitrary failures

This also provides significant improvements over modern cloud solutions providing a better way to securely manage IoT in smart cities. Currently, organizations are using cloud or a single server to store and process data. This often creates a single point of failure and reduces the confidentiality, integrity and availability of critical IoT. For example, confidentiality and privacy can be compromised when cloud/server is accessed by third parties that share the server. Integrity violations can occur at multiple levels. For example, the cloud server may return wrong data or could be compromised. Take for example, Heartbleed attack where CERTs were compromised. Finally, availability can be compromised if the single server or cloud instance is taken down. Next generation permissioned blockchain solutions – like Chios – solve these challenges. IoT device owners and users can specify who, when, and how the data is accessed. Blockchain servers can define access control rules (NIST, HIPAA, GPDR). Finally, fine grained access control can be programmed to assist with secure asset management. These innovative improvements in blockchain technology provide the imperative security, functionality and scalability that may give impetus to more distributed autonomous organizations.

Distributed Autonomous Organisations

Blockchain technology combines cryptography and distributed computing to provide a multiparty consensus algorithm to securely exchange value. Combining the disintermediation benefits of blockchain with the intelligence of smart contracts can help automate energy exchanges and give impetus to more distributed autonomous energy organisations (DAEO). DAEO may also help simplify and improve the efficiency of energy utilities by securely linking producers with consumers and creating prosumers with increased flexibility and control of how they generate, consume and exchange energy. Advances in blockchain and artificial intelligence (AI) continue to spur disruptive innovation, automating exchanges in value in new ways that are reducing the need for third-party trust mechanisms (Mylrea, 2018b).

These advances could help pave the way to a more distributed, autonomous and resilient infrastructures. This author is piloting a blockchain enabled microgrid controller that increases trustworthiness and integrity and helps enable peer-to-peer energy transactions. While grid modernisation has helped spur a more distributed and flexible smart grid, it has also created new challenges, such as, increasing the number of intermediaries involved in exchanging energy. Grid modernisation has also increased the cyber-attack surface through the increased use of smart energy devices that network, digitize, automate, and increasingly converge energy supplies in the cyber-physical energy supply chain. Blockchain or distributed ledger technology shows potential in identifying and monitoring these complex Internet IoT environments, characterised by an increasing number of critical cyber assets and data being exchanged in a complex energy value chain. Blockchain technology shows potential in overcoming some of these challenges needed to give impetus more distributed autonomous energy organizations (Mylrea, 2018b).

In the same way, the Internet transformed centralized organization to decentralized. Blockchain technology provides an innovative cryptographic proof that works as a distributed consensus algorithm to securely exchange and store value. As a result, today's smart decentralized cities will become more distributed as infrastructures become increasingly interoperable, networked and autonomous. Combining the disintermediation benefits of blockchain with the intelligence of smart contracts can help automate energy exchanges and give impetus to more distributed autonomous energy organizations (DAEO) providing an innovative new digital trust anchor to securely exchange and store value (Mylrea, Gourisetti, Bishop and Johnson, 2018).

Combining the disintermediation benefits of blockchain with the intelligence of smart contracts can help automate energy exchanges and give impetus to more distributed autonomous energy organisations (DAEO) providing an innovative new digital trust anchor to securely exchange and store value.

Breaking the Blockchain Immutability Myth

Cybersecurity is complex, non-linear and evolving. Blockchain and the data it protects will never be 100% secure. Change is a constant and nothing is immutable. Yet, something needs to change as both systems and policies have not kept up with the cyberthreats. Cybersecurity paradigms are antiquated. From a cybersecurity perspective, blockchain shows potential to help improve the following areas: identify management – providing a secure ledger of actions for vulnerable Internet of Things; configuration and patch management; and supply chain security – tracking through the entire chain of custody. While most cybersecurity solutions increase costs, reduce functionality and ease of use, blockchain solutions might provide a unique value proposition to both increase security and optimise systems.

While most cybersecurity solutions increase costs, reduce functionality and ease of use, blockchain solutions provide a unique value proposition to both increase security and optimise systems.

But with the prospect of improved cybersecurity also comes peril. A number of cybersecurity gaps remain: vulnerable code, bad deployments and misconfigurations of blockchain could actually create more cybersecurity challenges than solutions. A couple of these vulnerabilities have been exploited, resulting in significant economic and reputational damage: If you compromise 51% of the blockchain nodes, you can fork or manipulate the consensus algorithm. Vulnerabilities in crypto hot wallets make for excellent targets. It is similar to a bank advertising that it has no guards, no locks and all of the cash it holds is untraceable. Another cybersecurity gap is that malware or illegal data may be stored in the blockchain. Its immutability then possibly becomes a big problem. Quantum computing could also potentially decode the meta data stored in the blockchain hash, exposing information. The following graphic highlights common blockchain cybersecurity vulnerabilities:

Blockchain Considerations

Despite these challenges, blockchain's cybersecurity value proposition is real. Blockchains' consensus mechanisms provides a cryptographic proof for what, when, where, and with whom a transaction took place. This metadata is hashed and stored in a way that is inherently immutable. This removes the need for third-party intermediaries and supports moving towards more efficient and resilient organisations. However, blockchain is not a panacea. Potential users need to first decide if blockchain is the right solution to their problem. A number of blockchain solutions create more problems than answers, expand security gaps more than mitigate them, increase costs rather than efficiencies, increase rather than optimise latency, and increase energy use rather than reduce it. Blockchain solutions that help track and secure large data sets also need to be energy efficient, economic, and interoperable. Cost, functionality, scalability, and cyber-resilience are all important factors in considering the functional requirements.

Fig. 1. Common blockchain cyber vulnerabilities. Source: Mylrea & Gourisetti, 2018.

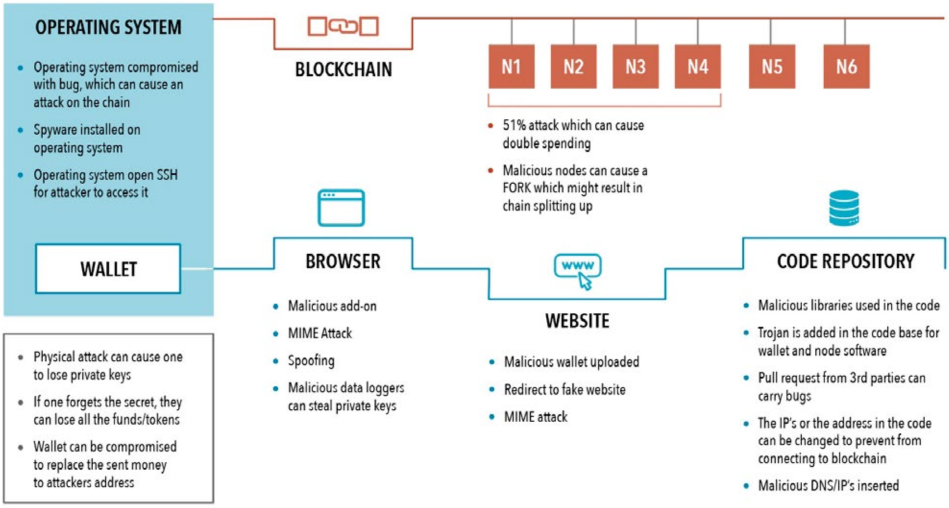
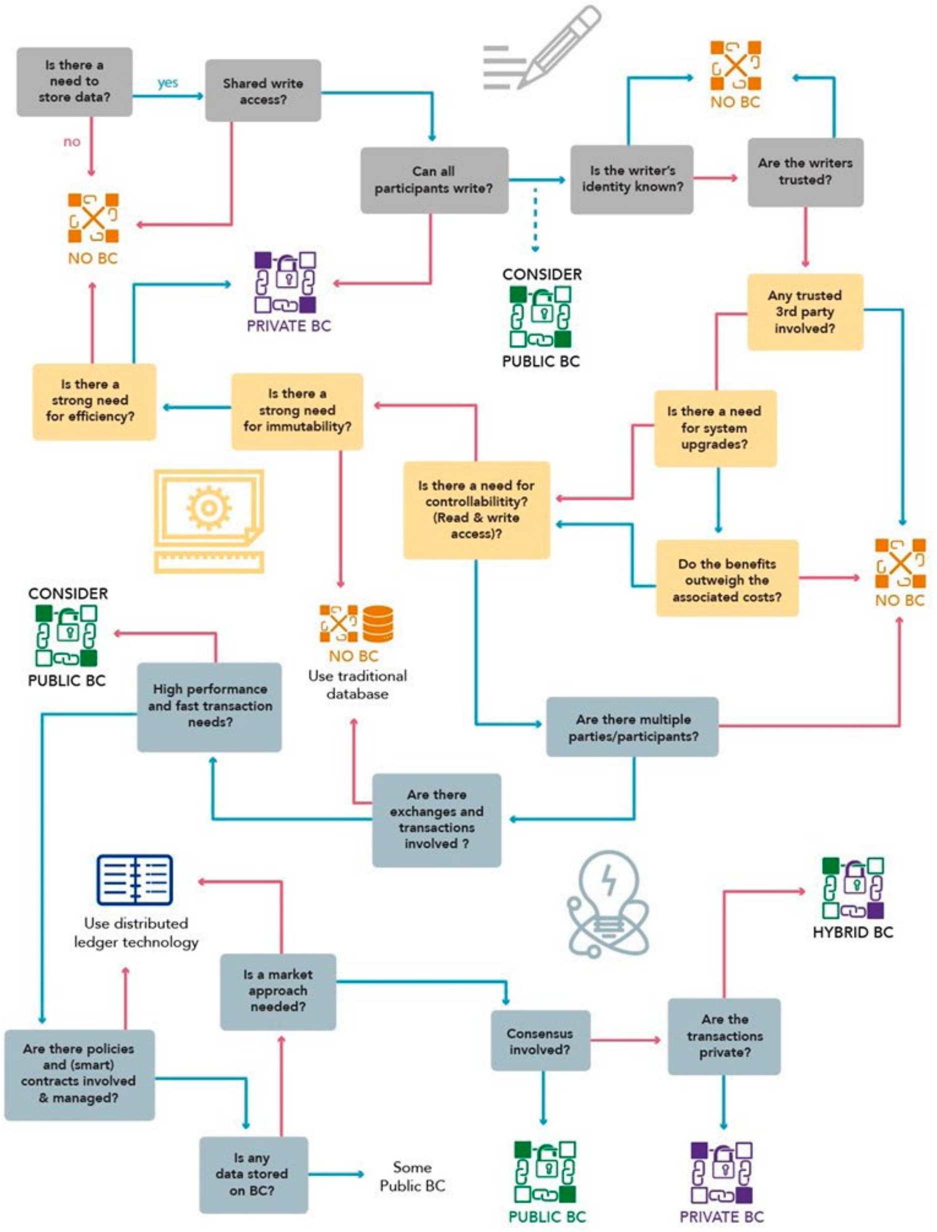

OPERATING SYSTEM
Operating system compromised with bug, which can cause an attack on the chain
Spyware installed on operating system
Operating system open SSH for attacker to access it
WALLET
Physical attack can cause one to lose private keys
If one forgets the secret, they can lose all the funds/tokens
Wallet can be compromised to replace the sent money to attackers address
BLOCKCHAIN
N1
N2
N3
N4
N5
N6
51% attack which can cause double spending
Malicious nodes can cause a FORK which might result in chain splitting up
BROWSER
Malicious add-on
MIME Attack
Spoofing
Malicious data loggers can steal private keys
www
WEBSITE
Malicious wallet uploaded
Redirect to fake website
MIME attack
CODE REPOSITORY
Malicious libraries used in the code
Trojan is added in the code base for wallet and node software
Pull request from 3rd parties can carry bugs
The IP's or the address in the code can be changed to prevent from connecting to blockchain
Malicious DNS/IP's inserted

Fig. 2. Blockchain Roadmap. Source: Mylrea & Gourisetti, 2018.


Is there a need to store data?
yes
no
Shared write access?
Can all participants write?
Is the writer's identity known?
Are the writers trusted?
NO BC
NO BC
CONSIDER
PUBLIC BC
PRIVATE BC
Any trusted 3rd party involved?
Is there a strong need for efficiency?
Is there a strong need for immutability?
Is there a need for system upgrades?
Is there a need for controllability? (Read & write access)?
Do the benefits outweigh the associated costs?
NO BC
CONSIDER
PUBLIC BC
NO BC
Use traditional database
High performance and fast transaction needs?
Are there multiple parties/participants?
Are there exchanges and transactions involved ?
Use distributed ledger technology
HYBRID BC
Is a market approach needed?
Are there policies and (smart) contracts involved & managed?
Consensus involved?
Are the transactions private?
Is any data stored on BC?
Some Public BC
PUBLIC BC
PRIVATE BC

Once it is determined that blockchain is the right solution, it is essential to map both the business and operational or technological requirements. Not all blockchains are created equal. Each has its own costs, latencies, interoperability challenges, etc. For smart city and critical infrastructure solutions, it is essential that the blockchain solution:

1. Prioritises security;
2. Is interoperable with different protocols;
3. Can make sub-second transactions and scale to a million users;
4. Is not cost prohibitive (Mylrea, Gourisetti, Bishop, & Johnson, 2018).

Conclusion

As the digitisation and networking of smart cities and infrastructures continues to expand the cyber-attack surface of IoT and global supply chains, new innovative solutions are needed to mitigate a complex and evolving cyber-physical threat. This paper examined how blockchain technology can help usher in a new cybersecurity paradigm through use of a cryptographic-signed distributed ledger that provides data provenance, attribution, and auditability. Indeed, blockchain provides a number of clear opportunities, challenges, and benefits worthy of future research and application to secure rapidly evolving smart cities and infrastructure and their array of vulnerable things. ■

About the author:

Michael Mylrea

Dr. Michael Mylrea is a Senior Advisor for Cybersecurity and Blockchain Lead and at Pacific Northwest National Laboratory. He has over 18 years of experience working on cybersecurity with leadership positions in industry and government. He leads several cybersecurity R&D and blockchain projects, including the largest federally funded blockchain cybersecurity project in the United States. He is also a Senior Cybersecurity Advisor to WA IoT Council, George Washington University (GWU) I3P and Rocky Mountain Institute. He completed his doctorate at GWU focused on cyber-resilience, graduate degrees and coursework at Tufts Fletcher School, Harvard Law School, WGU (MSIA), Tel Aviv University (Fulbright); and double majored at University of Wisconsin–Madison. Dr. Mylrea is proficient in several foreign and computer languages.

References

Daniel, A. (2018). Supply chain cyber-attacks hit two-thirds of firms. *Supply Management*. Retrieved from: https://www.cips.org/en/supply-management/news/2018/july/supply-chain-cyber-attacks-hit-two-thirds-of-companies.

Franco, P. (2014). *Understanding Bitcoin: Cryptography, Engineering and Economics*, John Wiley & Sons.

Mylrea, M. (2017). Smart Energy-Internet-Of-Things Opportunities Require Smart Treatment Of Legal, Privacy And Cybersecurity Challenges. *Journal of World Energy Law and Business*, 10, no. 2, pp. 147–158.

Mylrea. M. (2018a). *Blockchain – Technology that helps build trust?* Presentation at CYBERSEC 2018, Krakow, Poland.

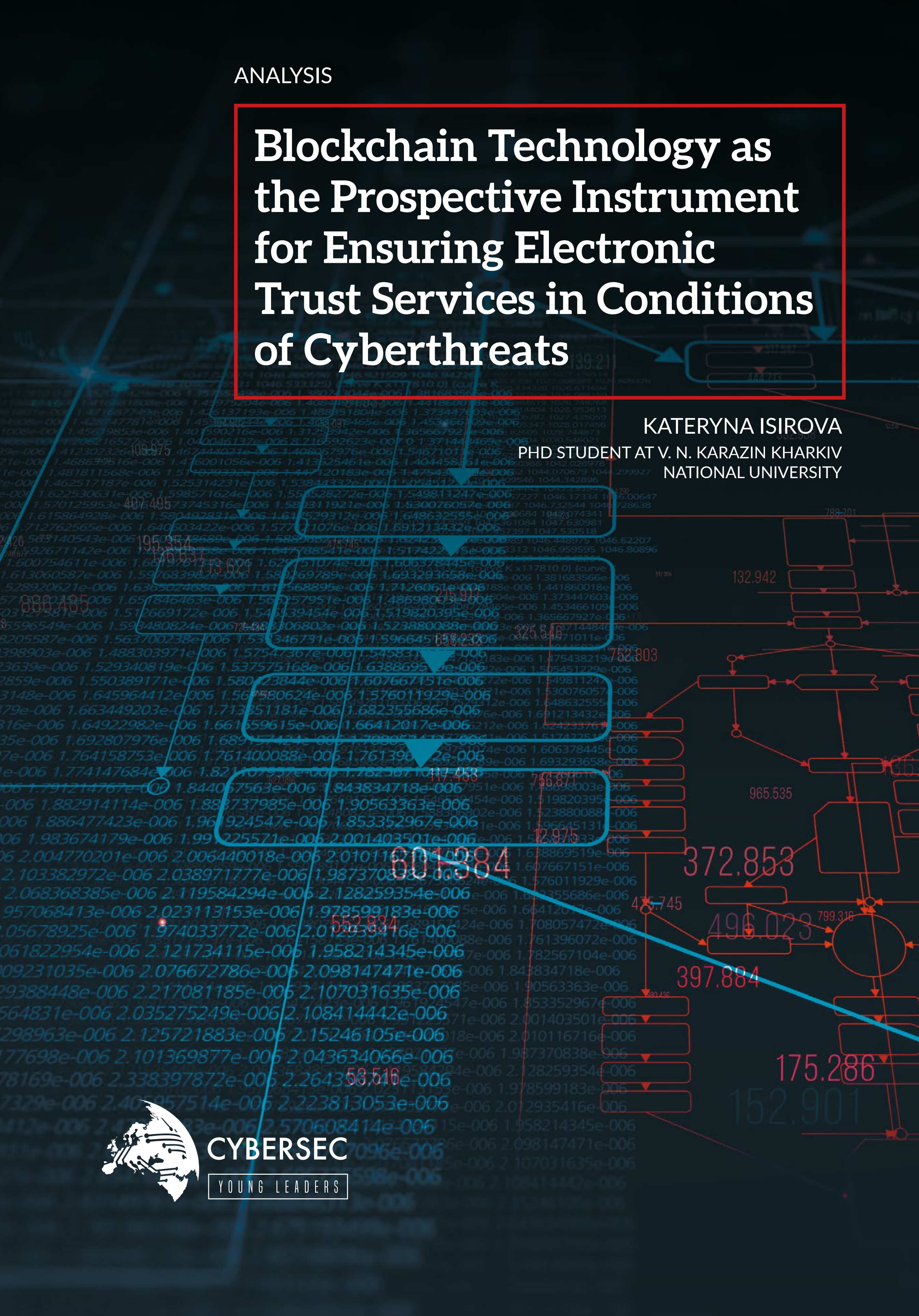
Mylrea. M. (2018b). *AI Enabled Blockchain Smart Contracts: Cyber Resilient Energy Infrastructure and IoT*. Paper presented at the 2018 AAAI Spring Symposium.

Mylrea, M., Gourisetti, S., Bishop, R., & Johnson, M. (2018). *Keyless Signature Blockchain Infrastructure: Facilitating NERC CIP Compliance and Responding to Evolving Cyber Threats and Vulnerabilities to Energy Infrastructure*. Paper presented at the IEEE PES Transmission & Distribution Conference & Exposition.

POA Network. (2017). Proof of Authority: consensus model with Identity of Stake. *Medium*. Retrieved from: https://medium.com/poa-network/proof-of-authority-consensus-model-with-identity-at-stake-d5bd15463256.

Tapscott, D., & Tapscott, A. (2016). *The Blockchain Revolution: How the Technology Behind Bitcoin Is Changing Money, Business, and the World*, Portfolio.

Walch, A. (2017). The Path of the Blockchain Lexicon (and the Law). *Review of Banking & Financial Law, 36*, pp. 713-765.



ANALYSIS

Blockchain Technology as the Prospective Instrument for Ensuring Electronic Trust Services in Conditions of Cyberthreats

KATERYNA ISIROVA
PHD STUDENT AT V. N. KARAZIN KHARKIV NATIONAL UNIVERSITY

CYBERSEC
YOUNG LEADERS

Introduction

For more than 15 years, the society has been introducing electronic technologies into its life. In the European Union, the corresponding Directive was adopted in 1999[1]. In 2012 the first regulation was proposed[2]. And finally, in July 2014 the new Regulation of the European Parliament and of the Council on electronic identification and trust services for electronic transactions in the internal market (eIDAS) was adopted. The main element for authenticity confirmation in the system of trust services in Europe is a digital (and within the terminology of the Regulation 2014 – electronic) signature.

Ukraine is actively moving towards the harmonisation with the Regulations requirements, as well as with the requirements of eIDAS in the field of electronic identification and electronic trust services. A great deal of forums, conferences, discussions concerning the system of electronic identification architecture and trust services implementation are taking place in Ukraine. In its regions, a large number of pilot projects in this area are being implemented.

The main objective of Ukraine is not only to deploy the full range of electronic trusted services, but also to ensure their interoperability and transboundarity. From this perspective, it is important to ensure legal, functional, and technological interoperability of electronic trusted services infrastructure in Ukraine with European systems. Building trust in the online environment is a key to economic and social development. Lack of trust makes consumers, businesses, and administrations hesitate to carry out transactions electronically and to adopt new services. To enhance the trust of all stakeholders and to promote the use of trust services and products, the notions of qualified trust services and qualified trust service provider should be introduced with a view to indicating requirements and obligations to ensure high-level security of whatever qualified trust services and products are used or provided.

Building trust in the online environment is a key to economic and social development. Lack of trust makes consumers, businesses, and administrations hesitate to carry out transactions electronically and to adopt new services.

Moreover, it should be noted that the solution to these issues and reliable operation of such systems acts as one of the foundations of state cybersecurity. Since the main goal of the cybersecurity strategy of Ukraine is to create a modern and flexible national system of cybersecurity to protect the state's national interests in the information sphere, solving these problems is urgent for Ukraine today.

Policy of Ukraine and main challenges

Neither successful implementation of modern technologies of electronic management nor electronic trust services are possible without the creation of an appropriate infrastructure. The infrastructure for implementing these technologies is the public key infrastructure (PKI). The use of electronic trust services and of a digital signature relies on the trust between the subjects of interaction, the public key infrastructure and is related to trust model implementation.

In Ukraine, active research in this area is conducted to reach the formulated objectives. Based on the results, practical decisions and corresponding architecture are being developed. In 2017 Ukraine adopted the Law of Ukraine On Electronic Trust Services, which defines the legal and organisational framework for the provision of electronic trust services, including cross-border services, the rights and obligations of subjects of legal relations in the field of electronic trust services, the procedure for implementing governmental supervision

[1] Directive 1999/93/EC of the European Parliament and of the Council of 13 December 1999 on a Community framework for electronic signatures

[2] Proposal for a Regulation of the European Parliament and of the Council on electronic identification and trust services for electronic transactions in the internal market – COM/2012/0238 final - 2012/0146 (COD).

(control) for compliance with the requirements of legislation in the field of electronic trust services, as well as legal and organizational basis for the implementation of electronic identification. For the effective use and high-quality provision of such services, it is necessary to solve many technological and technical problems. Moreover, advances in the field of quantum computing are an important challenge for modern information security as a whole and for cryptography in particular. The rapid evolution of quantum computers and the resulting computation speed increase entail new risks for existing cryptographic systems. In 2004 the architecture of PKI was implemented in Ukraine, which became the basis for the use of public key technology and the provision of services for cryptographic key management. This architecture is a hierarchical system. In addition to the hierarchical architecture, there are still a number of possible uses that PKI has not been put to due to the impossibility of reliable trust model implementation.

> **Neither successful implementation of modern technologies of electronic management nor electronic trust services are possible without the creation of an appropriate infrastructure.**

The purpose of this paper is to offer a new concept for PKI development using blockchain technology.

Hierarchical Public Key Infrastructure. Characteristics and issues

Public Key Infrastructure (PKI) is a set of tools (technical, material, human, etc.), distributed services, and components, which are collectively used to support cryptographic tasks based on private and public keys (ISO/IEC 9594-8).In fact, PKIs are based on several basic principles (PKI: tutorial, 2011):

- Private Key is known only to its owner.
- Certification Authority (CA) creates an electronic document – a public key certificate, thus certifying the fact that the private key is known exclusively to the owner of the certificate; the public key is freely transferred in the certificate.
- Nobody trusts each other, but everyone trusts CA.
- CA confirms or refutes that the public key belongs to the given person who owns the corresponding private key.

The main regulating document is ITU-T X.509 Privilege Management Infrastructure standard (ISO/IEC 9594-8). It defines data formats and public key distribution procedures using appropriate certificates with electronic signatures. These certificates are provided by CA. In addition, ISO/IEC 9594-8 defines certificate revocation lists (CRL) format, attribute certificates format, and certification path validation algorithm.

The main threats for such type of systems are:

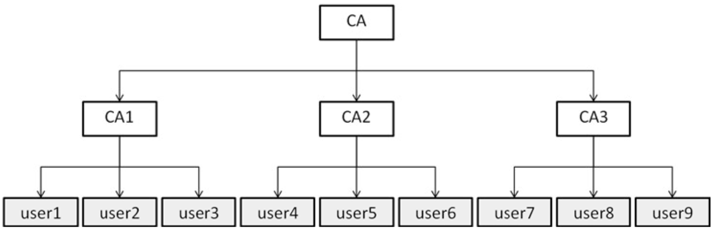
- refusal to perform actions;
- certificate forgery.

To ensure trust, it is necessary to ensure the functioning of the system within the framework of the actual trust model. X.509 offers to use the following trust models:

- strict hierarchy of CAs;
- loose hierarchy of CAs;
- policy-based hierarchy;
- distributed trust model;
- four-corner trust model;
- user-centric model;
- web trust model.

The overwhelming majority of PKIs today is based on strict CA hierarchy (Fig. 1).

Fig. 1. Strict hierarchy of CAs.
Source: Recommendation ITU-T X.509, 2017



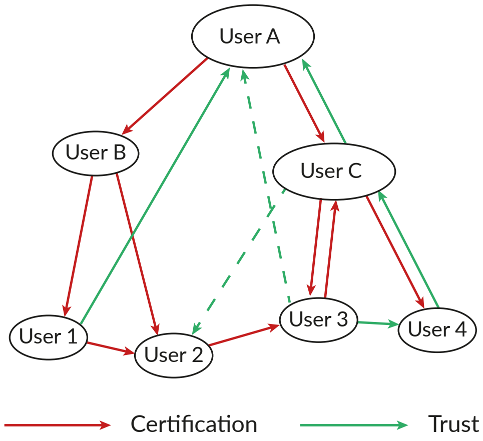
However, such structure has a number of drawbacks (Isirova and Potii, 2018):

- Security of the whole system depends on CA root certificate. In the case of its compromise, all certificates in the system are compromised.
- Users do not actually dispose of their identity. They need to contact CA whenever their keys have to be generated again.
- Interoperability is lacking. Certificates issued by different CA cannot be used in parallel.
- There is no one-to-one correspondence between the user and the certificate since many certificates can be issued for one user.

Other trust models are poorly distributed or not used at all. However, the analysis showed that with the new blockchain technology other trust models can be reliably implemented, in particular the user-centric model.

The user-centric model (ISO/IEC 9594-8) is illustrated by the well-known Pretty Good Privacy system (Fig. 2).

Fig. 2. User-centric trust model.
Source: Recommendation ITU-T X.509, 2017



In such a system the user is responsible for deciding which certificates she or he considers secure and which insecure. The primary source of trust is relatives' or friends' certificates, i.e. those whom the user knows personally (i.e. the initial identification is carried out by the user himself). Due to its dependence on user actions, such a system could only be used in a highly specialised and high-tech community. But it was not viable in a broad community in which users do not have a sufficient level of knowledge about information technology and security. Moreover, this model cannot be used in government or financial sector where it is important to control interaction between users.

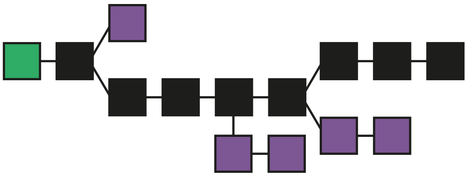
Further in the paper, a solution to avoid this disadvantage with the help of blockchain technology will be offered.

Confidence-providing blockchain features that make it applicable in an environment of mistrust

In our opinion blockchain technology is able to provide the confidence in the system unaided. A blockchain is a continuously growing list of facts, called blocks, which are linked and secured using cryptography (Nielsen, 2013). Facts can be anything, from money transactions to content signing. A blockchain database is managed autonomously using a peer-to-peer network and a distributed time-stamping server. Such a structure allows the participants to verify and audit transactions inexpensively (The Economist, 2015; Armstrong, 2016).

Transaction is regarded as confirmed if its format and signatures are verified and if such a transaction is linked in block with several others.

Fig. 3. Blockchain formation. Source: Nielsen, 2013



When a node wants to add a fact to the log, a consensus is formed in the network to determine where this fact should appear in the log; this consensus is called a block (Catalini and Gans, 2016).

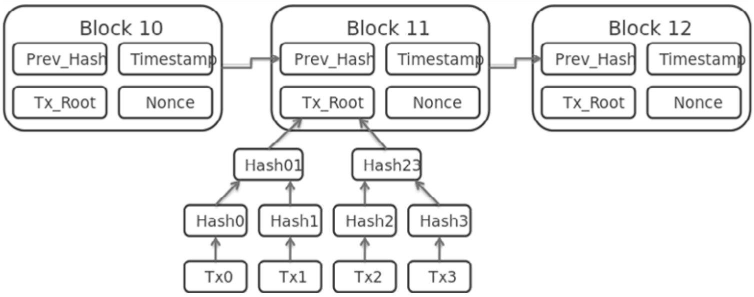
The block content can be checked, since each block contains information about the previous one. All the blocks are lined up in a single chain (Fig. 3), which includes information about all transactions that have been performed at any time in the database.

The very first block in the chain (the genesis block) is considered a separate case, since it does not have a parent block. This makes it possible to exploit it for record management activities, for instance documenting provenance, identity management, voting etc. (Ekblaw et al., 2016).

A blockchain is a continuously growing list of facts, called blocks, which are linked and secured using cryptography. Facts can be anything, from money transactions to content signing. A blockchain database is managed autonomously using a peer-to-peer network and a distributed time-stamping server.

The block consists of a header and a list of transactions (Fig. 4). The block header includes its hash, the previous block hash, the transaction hash, and additional service information. Transactions in the block are hashed and encoded into a Merkle tree, similar to hash generation for a file in the BitTorrent protocol. The linked blocks form a chain (Catalini and Gans, 2016; Tapscott and Tapscott, 2016; Trottier, 2016).

Fig. 4. Block structure. Source: Nielsen, 2013.



Blocks are simultaneously produced by several "participants". Confirmed blocks are sent to the network, including in a distributed base of blocks. The situations when several new blocks in different parts of a distributed network call the same previous block can arise. Because of that, a chain of blocks can be broken into branches (Narayanan et al., 2016). Specifically or accidentally, it is possible to limit the retransmission of information about new blocks (for example, one of the chains can evolve within the local network).

When the retransmission is restarted, the participants should reach consensus as to which branch is correct. It is possible with the use of decentralised consensus protocols. The basic requirements for consensus protocols are:

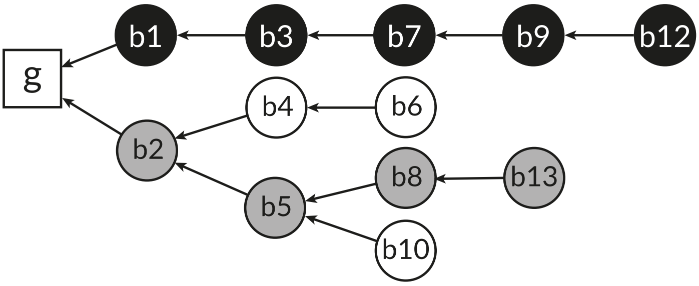
- Central trust point is absent.
- Nodes are equal.
- The majority of nodes are "honest".
- "Honest" participants do not know which nodes are controlled by intruders.
- The system functions in an unreliable network (network failure, packet loss).

Consensus protocols can be classified into several groups:

- Proof of Work Protocols (PoW Protocols). These protocols suppose that participants make their decisions on the basis of the length of the branch (as in the Bitcoin network). But there is a problem connected with transaction loss. To counteract this issue, there are new algorithms such as GHOST (Fig. 5), which uses a tree-like structure instead of the linear structure to help reduce the number of lost transactions.

Fig. 5. GHOST algorithm consensus protocol. Source: Kiayias and Panagiotakos, 2016.

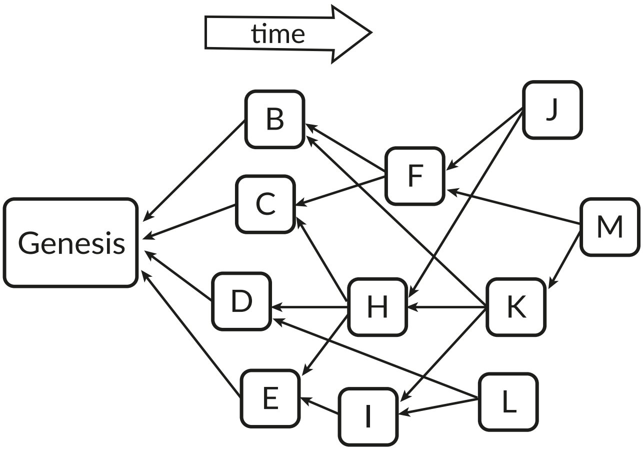
- **Proof of Stake Protocols (PoS Protocols).** In fact there is a voting procedure (Fig. 7). Such type of protocol logic is built so that for the participant there is no more advantageous strategy than following the protocol honestly
- **Byzantine Fault Tolerance Protocols (BFT Protocols).** They historically appeared first and are based on the Byzantine agreement problem. BFT protocols required more than 2/3 honest nodes, but they have high capacity.
- **Alternative Consensus Protocols.** For example, Proof of Activity Protocol, Proof of Burn Protocol, and other hybrid protocols.



Algorithms SPECTRE and PHANTOM (Fig. 6) use unidirectional cyclic graph to avoid lost transactions altogether (Sompolinsky and Zohar, 2017).

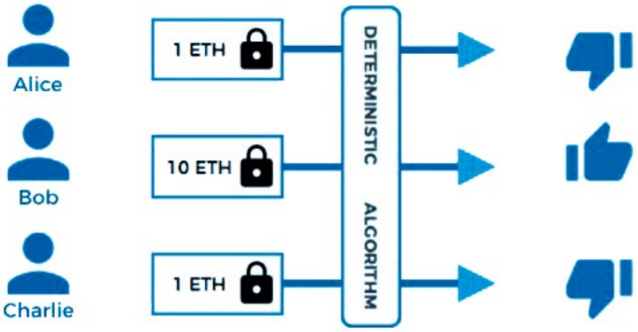
Fig. 6. PHANTOM algorithm consensus protocol. Source: Sompolinsky and Zohar, 2017.

Due to its open nature, a chain of blocks allows an intruder to make changes to an arbitrary block. But then the attacker needs to recalculate the hash not only of the modified block, but of all subsequent ones. In fact, computational power for this operation will not be lower than the one



used to create the modified and subsequent blocks (i.e., all current power), which makes this possibility extremely unlikely (Nielsen, 2013; The Economist, 2015; Armstrong, 2016).

Fig. 7. PoS algorithms consensus protocol. Source: Daian et al., 2016.



Example of using Blockchain technology for PKI development

This idea can be applied for PKI without a strict CA hierarchy construction.

The basic principles of decentralised PKI have been formulated (Isirova and Potii, 2018). They are as follows:

- Each user (the user acts as a node) stores his key pair on their own. The public key certificate is sent along with the signed message.
- Records about a transaction are stored in a distributed database according to the blockchain canons.
- Transaction block contains the certificate status register.
- When verifying the transaction validity (in fact, the validity of the public key certificate), the auditor needs to trace the status register of the sender's certificate until its first publication.
- However, initial identification of a new user is mandatory and must be reliably confirmed. For this and only this purpose, a trusted node (an analogue of the certification authority in a hierarchical structure) is needed. Its role will consist in new user's certificate initial release. After the first transaction made by this user, the request to the trusted node no longer occurs. That is, this node will provide new users with a "parent" block ("genesis block"). Existing nodes can check the new user's certificate status. It seems appropriate to assign this role to the state structure.The following notation is introduced:

M – message
Sign – sender's electronic signature
H – cryptographic hash function
Sert – sender's public key certificate
ID – sender's unique identifier, given to him at initial identification
Status – status of the sender's public key certificate.

As mentioned above, the initial identification should be carried out by the state structure (trusted node). The user first applies to the trusted node.

When verified, the user will be given a unique identifier (ID) and the corresponding public key certificate (Sert). It should be noted that the trusted node does not store the user ID, in fact, it does not know it.

After passing through the initial identification, data are spread in a distributed database where they are stored in following form (Table 1).

Table 1. Distributed Database. Source: Isirova and Potii, 2018

H(Sert,ID)	*H(Sert,Status)*	*Status*
...	...	...

Signature generating algorithm does not differ from the existing one and depends only on the type of signature used.
The sender generates the next transaction:

M; Sign; H(Sert,ID); Sert; Status

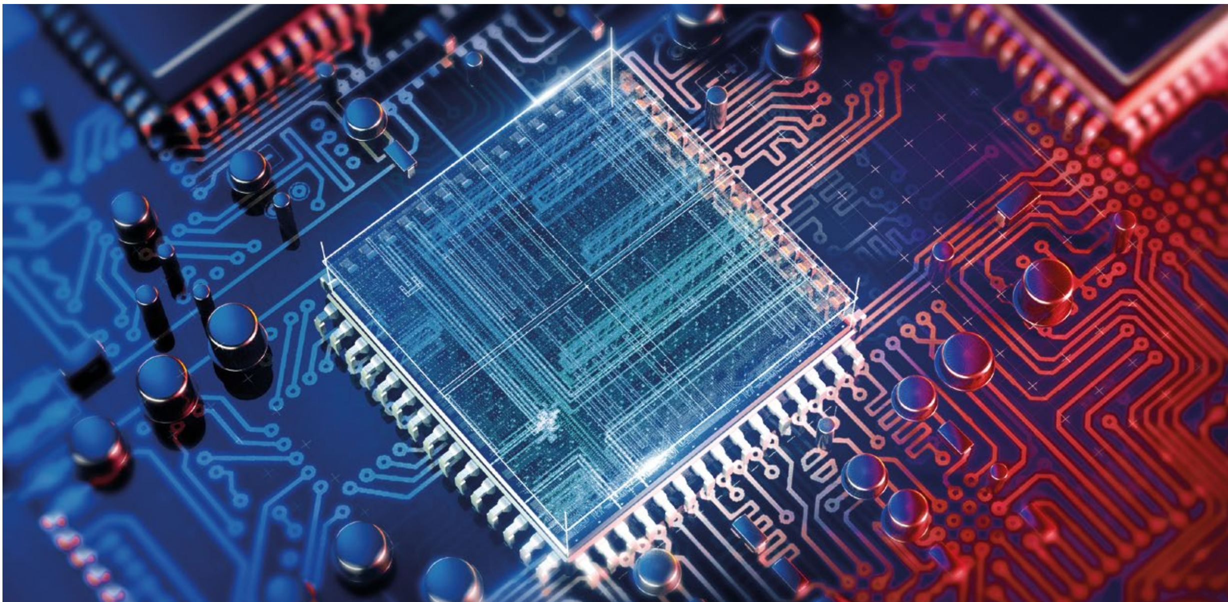
The verification algorithm consists of two stages: The first stage is to verify the electronic signature *(Sign)* based on the sender's public key certificate *(Sert)*.
If this verification is successful (that is, the electronic signature is generated using the private key that corresponds to the provided sender's public key certificate), you should move to the second stage. Verifying whether the sender's public key certificate does belong to the sender.

The second stage consists of the following steps (Isirova and Potii, 2018):

- Get the value and address of the field Status from the table based on H(Sert, ID) received from the sender.
- Calculate H1(Sert, Status).
- Get the value and address of the field Status1 from the table based on H1 (Sert, Status).
- If the value and address of H and H1 are equal, the verification is considered successful.

The system proposed above has several advantages (Isirova and Potii, 2018):

- It considerably reduces the cost of maintaining a cumbersome hierarchical structure of CA.
- Users independently control their identification data and are able to immediately report the need for their correction (compromise).
- The "man in the middle" threat is lessened. The intruder will need to attack the entire system; accordingly, in order to have a 50% chance of success in solving one block, he or she will need to have the computing power equal to the processing power of the rest of the system;
- Directed attack targets disappear. In contradistinction to hierarchical structure, where the main targets for the attackers are CAs, in this case there is no clear target for the attack, because the information is stored in distributed form and the attacker is actually forced to attack the whole network, not a specific node.
- The proposed system can be used not only for the electronic signature service, but also for ensuring electronic identification.
- The collapse of one or more nodes does not result in system shutdown.
- There is no need to make and store backups.
- System interoperability relies on the fact that certificates issued by various CAs can easily be used in a single system.
- Scalability is easy to achieve, because adding a new user (a new node) occurs without changing the basic principles of the architecture.



Conclusions

1. Nowadays progress in the field of electronic technologies allows for providing more efficient electronic trust services.
2. Since Ukraine chose to harmonise its national electronic trust services system with European systems, an important aspect is to ensure legal, functional, and technological interoperability of electronic trust services infrastructure in Ukraine with European systems.
3. It is necessary to take into account the new challenges that are dictated by the development of quantum technologies in the construction of promising systems and infrastructures.
4. Taking into account the above-mentioned, blockchain technology looks to be a prospective mechanism for reaching the objectives which are set. The analysis showed that PKI based on the blockchain technology security will exceed the centralised system security. It should be understood that this is not about cryptographic security, but about system resilience. The application of the above approach will facilitate the transition to new signature algorithms, in particular to the post-quantum ones, in which the stability does not depend on the cryptographic key validity period (3 years, 5 years), but on the number of overlays (for example, hash-based signatures). Thus, blockchain technology will allow more rational public key certificate management.
5. Energy costs required for the implementation of the attack on the system will be 50% of the computing power of the system. The intruder will need to attack the entire system. Accordingly, in order to have a 50% chance of success in solving one block, he or she will need to have a computing power equal to the processing power of the rest of the system. In addition, the recommendation of 3 to 5 confirmation steps dramatically and significantly reduces the chances. Thus, the stability of the system increases with the increase in the number of nodes (users). Such property of the system is valuable in the situation of cyberattacks. ■

About the author:

Kateryna Isirova

PhD Student at V. N. Karazin Kharkiv National University, Computer science department. Research field: information security, post-quantum cryptography.

References

Armstrong, S. (2016). Move over Bitcoin, the blockchain is only just getting started. *Wired*. Retrieved from: https://www.wired.co.uk/article/unlock-the-blockchain.

Catalini, C., Gans, J. S. (2016). Some Simple Economics of the Blockchain. Rotman School of Management Working Paper No. 2874598, MIT Sloan Research Paper No. 5191-16.

Daian, P., Pass R., Shi, E. (2016). Snow White: Provably Secure Proofs of Stake. Retrieved from: https://eprint.iacr.org/2016/919.pdf.

Ekblaw, A., Azaria, A., Vieira T., Lippman, A. (2016). MedRec: Medical Data Management on the Blockchain. Conference Paper: 2nd International Conference on Open and Big Data.

Isirova, K., Potii, O. (2018). Decentralized Public Key Infrastructure Development Principles. The 9th IEEE International Conference on Dependable Systems, Services and Technologies.

ISO / IEC 9594-8 and ITU-T X.509. (2017). Information technology – Open Systems Interconnection – The Directory – Part 8: Public-key and attribute certificate frameworks.

Kiayias, A., Panagiotakos, G. (2016). On Trees, Chains and Fast Transactions in the Blockchain. Retrieved from: https://eprint.iacr.org/2016/545.pdf.

Narayanan, A., Bonneau, J., Felten, E., Miller, A., Goldfeder, S. (2016). Bitcoin and Cryptocurrency Technologies: a Comprehensive Introduction. Princeton: Princeton University Press.

Nielsen, M. (2013). How the Bitcoin protocol actually works. Retrieved from: http://www.michaelnielsen.org/ddi/how-the-bitcoin-protocol-actually-works/.

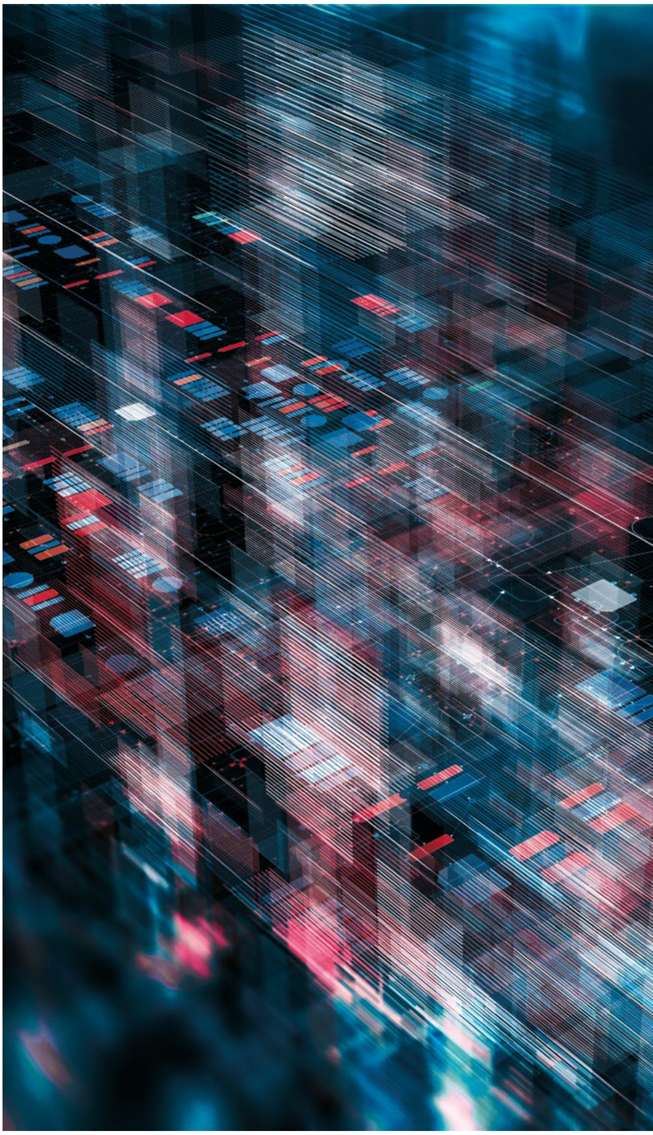
PKI: technology, architecture, construction and implementation: a tutorial / Potiy AV, Lenshin AV Soroka LS, Esin VI Moroz BI - Dnepropetrovsk: Akadimiya border service of Ukraine 2011.

Sompolinsky, Y., Zohar, A. (2017). PHANTOM, GHOSTDAG: Two Scalable BlockDAG protocols. Retrieved from: https://eprint.iacr.org/2018/104.pdf.

Tapscott, D., Tapscott, A. (2016). Here's Why Blockchains Will Change the World. *Fortune*. Retrieved from: http://fortune.com/2016/05/08/why-blockchains-will-change-the-world/.

The Economist. (2015). Blockchains: The great chain of being sure about things. *The Economist*. Retrieved from: https://www.economist.com/briefing/2015/10/31/the-great-chain-of-being-sure-about-things.

Trottier, L. (2016). Original-bitcoin (a historical repository of Satoshi Nakamoto's original bitcoin source code). *Github*. Retrieved from: https://github.com/trottier/original-bitcoin.

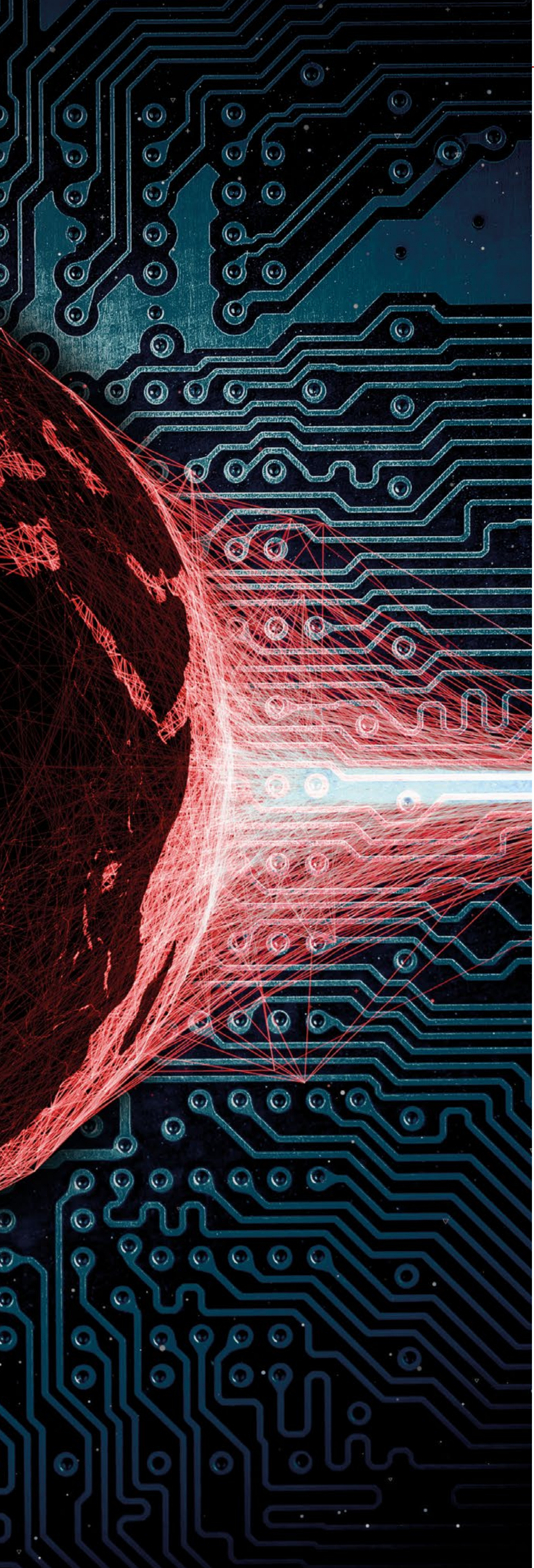


ANALYSIS

The (un)desirable consequences of the (extra)territorial scope of the General Data Protection Regulation

ISABELLA OLDANI
PHD CANDIDATE AT THE UNIVERSITY OF TRENTO

CYBERSEC
YOUNG LEADERS



1. Introduction

One of the greatest challenges posed by cyberspace is to determine the territorial boundaries of national jurisdictions. The widespread and ever-increasing use of the technology on which cyberspace is based has, in fact, challenged States' capability to exert their jurisdiction in the "borderless cyber world" (Sachdeva, 2007, p. 245). Issues of conflicting laws and enforceability problems are bound to emerge when States attempt to unilaterally expand their jurisdictional claims over a dimension of such an indefinite nature. Data protection law is one of the fields where similar issues have emerged or, at least, will emerge, especially considering the extraterritorial reach of the EU data protection legislation.

> **The widespread and ever-increasing use of the technology on which cyberspace is based has, infact, challenged States' capability to exert their jurisdiction inthe "borderless cyber world".**

This article will hence first analyse the concept of extraterritoriality as one of the main features of Regulation 2016/679 (hereafter GDPR or Regulation)[1] and of Directive 95/46/EC (hereafter Directive)[2] before it. In order to understand how these extraterritorial claims are shaped in practice, I will then analyse the territorial scope of the Regulation with a focus on the interpretative challenges and consequent legal uncertainties that arise when delving into the key terms in which the (extra)territorial scope of the EU data protection legislation is grounded. Before concluding, I will analyse the conflicts of laws and the enforceability problems that may arise

[1] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), OJ L119/1.

[2] Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, OJ L281/31.

as a consequence of the unilateral expansion of the EU data protection legislation across borders.

2. The Concept of Extraterritoriality

The extraterritoriality of the Regulation, and of the Directive before it, is often mentioned as one of the main features of the EU data protection legislation. However, there is no widely accepted definition of extraterritorial jurisdiction and even when a definition is adopted, drawing a line between territorial jurisdiction and extraterritorial jurisdiction can be highly challenging.

A useful definition of extraterritorial jurisdiction is provided by the International Law Commission: "[t]he assertion of extraterritorial jurisdiction by a State is an attempt to regulate by means of national legislation, adjudication or enforcement the *conduct of persons, property or acts beyond its borders* which affect the interests of the State in the absence of such regulation under international law".[3] Along the same lines, Senz and Charlesworth recalled that "[t]he term 'extraterritoriality' is generally understood to refer to the exercise of jurisdiction by a state over *activities* occurring *outside* its borders". More precisely, "[t]he traditional international legal use of the term 'extraterritorial legislation' covers two different types of laws: legislation that regulates the *conduct of nationals abroad*, and laws that apply to *conduct by non-nationals outside* the territory of the legislating country" (2001, p. 72, italics mine).

I argue that when determining whether a jurisdictional claim is extraterritorial or not (or at least, attempting to) in the data protection arena, the focus should not be on the location of the (data processing) *activities* but on the location of the natural or legal *person* that conducts those activities since "[p]ersons, whether legal or natural, are always located somewhere, while locating 'activities' may be more difficult" (Svantesson, 2014, p. 60). The focus on persons that process personal data rather than on the processing activity itself seems particularly sensible if one considers that, especially in the context of cloud computing, pinpointing the location(s) of the processing activities may be an impossible task.

To stress this "shift" of focus, for the purpose of this article I will adopt the definition of extraterritoriality suggested by Svantesson: "[a]n assertion of jurisdiction is extraterritorial as soon as it seeks to control or otherwise directly affect the activities of an *object* (person, business, etc.) *outside* the territory of the state making the assertion" (2014, p. 60, italics mine).

The focus on persons that process personal data rather than on the processing activity itself seems particularly sensible if one considers that, especially in the context of cloud computing, pinpointing the location(s) of the processing activities may be an impossible task.

3. Grounds for the Applicability of the EU Data Protection Legislation

The grounds that under the GDPR trigger the applicability of the EU data protection law are spelled out in Article 3. Precisely, the Regulation applies (1) "to the processing of personal data in the context of the activities of an establishment of a controller or a processor in the Union, regardless of whether the processing takes place in the Union or not" (establishment criterion); (2) "to the processing of personal data of data subjects who are in the Union by a controller or processor not established in the Union, where the processing activities are related to: (a) the offering of goods or services, irrespective of whether a payment of the data subject is required, to such data subjects in the Union; or (b) the monitoring of their behaviour as far as their behaviour takes place within the Union" (targeting criterion); (3) "to the processing of personal data by a controller not established in the Union, but in a place

[3] Report of the International Law Commission, Fifty-eighth session. (1 May–9 June and 3 July–11 August 2006). UN Doc. A/61/10, Annex E, para. 2 (italics mine). Retrieved from: http://legal.un.org/ilc/documentation/english/reports/a_61_10.pdf.

where Member State law applies by virtue of public international law".[4]

The following main differences can be identified between the territorial scope of the Directive and the territorial scope of the Regulation. Firstly, under the Regulation the establishment criterion does not refer exclusively to the establishment of a controller but also to the establishment of a processor.[5] Secondly, the targeting criterion has replaced the equipment criterion established under Article 4(1)(c) of the Directive which prescribed the applicability of the EU data protection legislation in the event that a controller not established in the EU "makes use of equipment, automated or otherwise, situated on the territory of" the Union for the purposes of processing personal data.

Under the Directive, the purpose of such a broad application was "primarily to ensure that individuals are not deprived of the protection to which they are entitled under the Directive, and, at the same time, to prevent circumvention of the law".[6] The intent to guarantee a comprehensive application of the system of protection laid out under the EU data protection legislation seems to also underpin the wording adopted in Article 3 of the GDPR since it retains and, to some extent, broadens the scope of application of the EU data protection law.[7] The analysis below will, however, show that this broad applicability of the EU data protection legislation also comes with several legal uncertainties.

Under the Directive, the purpose of such a broad application was "primarily to ensure that individuals are not deprived of the protection to which they are entitled under the Directive, and, at the same time, to prevent circumvention of the law".

3.1 Untangling the Establishment Criterion

The establishment criterion under Article 3 of the GDPR essentially replicates the first jurisdictional nexus introduced under Article 4(1)(a) of the Directive. For this reason, several considerations that have been expressed with reference to the key terms of the establishment criterion under the Directive can be extended to the Regulation.

Firstly, a correct understanding of the concept of "establishment" seems to be of primary importance. In this respect, it should be noted that Article 3 of the Regulation, like Article 4 of the Directive, does not refer to *the* establishment of the controller (or of the processor) but, more generally, to *an* establishment. This indicates that the attention of the EU co-legislators is not, or at least is not only, on the place of formal registration of a parent company, but also on any secondary establishments, such as subsidiaries, branches, and agencies.[8] Moreover, Recital 19 of the Directive, that is now transposed in Recital 22 of the Regulation, provides that "[e]stablishment implies the effective and real exercise of activity through stable arrangements". This broad wording adopted under Recital 19 of the Directive has been leveraged by the European Court of Justice (ECJ) for justifying a flexible interpretation of the concept of "establishment" (de

[4] Considering its lack of strong practical significance, I will skip the analysis of the cases where the Regulation applies by virtue of public international law.

[5] Article 4(1)(a) of the Directive prescribed the applicability of the EU data protection legislation where "the processing is carried out in the context of the activities of an establishment of the *controller* on the territory of the Member State; ..." (italics mine). Pursuant to Article 3(1) of the GDPR, the Regulation applies to the processing of personal data in the context of the activities not only of an establishment of a controller but also of an establishment of a processor in the Union.

[6] Article 29 Data Protection Working Party. (16 December 2010). *Opinion 8/2010 on applicable law.* WP 179, 9 (hereafter cited as WP 179).

[7] European Data Protection Board. (16 November 2018). *Guidelines 3/2018 on the territorial scope of the GDPR (Article 3)* – Version for public consultation (hereafter cited as Guidelines 3/2018): "Article 3 of the GDPR reflects the legislator's intention to ensure comprehensive protection of EU data subjects' rights and to establish, in terms of data protection requirement, a level playing field for companies active on the EU markets, in a context of worldwide data flows" (p.3). These guidelines are open to public consultation until 18 January 2019.

[8] See, Recital 19 of the Directive and Recital 22 of the GDPR.

Hert & Czerniawski, 2016, p. 233). In *Weltimmo*,[9] in particular, the ECJ noted that both the degree of stability of the arrangements and the effective exercise of activities through those arrangements "must be interpreted in the light of the specific nature of the economic activities" conducted by the undertaking in question, especially when it comes to companies that offer services only over the Internet.[10] In the light of this, even "the presence of only *one representative* can, in some circumstances, suffice to constitute a stable arrangement if that representative acts with a sufficient degree of stability through the presence of the necessary equipment for provision of the specific services"[11] and the "real and effective activity" exercised through stable arrangements may also be *minimal* ones.[12] Consistently, the European Data Protection Board (EDPB) has warned that even the presence of one single employee may constitute an establishment within the meaning of the GDPR.[13] However, besides recalling previous case law on the concept of establishment, the EDPB did not provide further guidance on the factors that should be considered in practice when assessing whether a controller or a processor has an establishment in the Union.

This flexible interpretation of the notion of "establishment" is certainly motivated by a laudable purpose: ensuring an effective and complete protection of data subjects' rights.[14] However, flexible interpretations are often developed at the expense of clarity. Indeed, although theoretically all companies (should) know where they are established and (should) hence know when their activities are subject to EU law, determining whether an "arrangement" can be counted as an establishment within the EU data protection legislation may raise several practical challenges when the boundaries of the notion of establishment are so loose.

For example, it is unclear whether a data centre represents an establishment within the scope of the EU data protection legislation. Indeed, unlike a server that "is simply a technical facility or instrument for the processing of information",[15] a data centre "comprises a building, normally with employees to maintain the servers, power, cooling, physical security, and so on" (Hon, Hörnle, & Millard, 2013, p. 232). Lack of clarity in the definition of this concept has also led to an inconsistent implementation of the establishment criterion across the Union, where the interpretation developed in some countries is more expansive than the one adopted in others (Kuner, 2003, p. 66).

As a further element of complexity, the GDPR, like the Directive before it, does not require that the data processing in question is conducted *by* the establishment itself. The application of the GDPR is, indeed, triggered whenever the processing of personal data is carried out "in the context of the activities of" an EU establishment of a controller or a processor. The words "in the context of the activities of an establishment" that have been transposed from the Directive to the Regulation need some clarification. Again, in *Google Spain*,[16] the ECJ showed its inclination to adopt a flexible interpretation of this notion. The central question raised in *Google Spain* was whether, under the Spanish data protection law implementing the Directive, the operator of the search engine (i.e. Google Inc.) could be requested to remove information about a person from the list of results displayed after a search made on the basis of the person's name, considering that Google Inc. has its seat in the United States and that its Spanish subsidiary, Google Spain, is a commercial agent for the Google group, selling advertising space mainly to undertakings based in Spain.

[9] Judgment of 1 October 2015, *Weltimmo*, C-230/14, ECLI:EU:C:2015:639.

[10] Ibid., para. 29.

[11] Ibid., para. 30 (italics mine).

[12] Ibid., para. 31.

[13] Guidelines 3/2018, 5.

[14] *Weltimmo*, para. 30.

[15] WP 179, 12.

[16] Judgment of 13 May 2014, *Google Spain and Google*, C-131/12, ECLI:EU:C:2014:317 (hereafter cited as *Google Spain*).

In compliance with the establishment criterion, in order to establish whether Google Inc. was subject to the EU data protection legislation, the ECJ had to establish whether "the processing of personal data for the purposes of the service of a search engine such as Google Search, which is operated by an undertaking that has its seat in a third State" (i.e. Google Inc.), was conducted in the context of the activities of its establishment in the EU (i.e. Google Spain).[17]

The ECJ gave a positive answer to this question on the basis of the fact that "the activities of the operator of the search engine [Google Inc.] and those of its establishment situated in the Member State concerned [Google Spain] are *inextricably linked*".[18] Indeed, on the one hand, Google Inc. could not perform its activities as an operator of a search engine without the profits gained through the selling of advertising space carried out by Google Spain; on the other hand, the search engine itself is, in turn, the means that allows Google Spain to perform its activities since the display of personal data on a search results page "is accompanied, on the same page, by the display of advertising linked to the search terms".[19]

The connection with the EU territory as a trigger for the applicability of the EU data protection legislation – represented by the presence of an establishment within the EU – was hence loosened by the ECJ in order to meet the objective of the Directive, i.e., ensuring "*effective* and *complete* protection of the fundamental rights and freedoms of natural persons, and in particular their right to privacy, with respect to the processing of personal data".[20] In order to achieve this objective, the EDPB has also recommended an extensive interpretation of the words "in the context of the activities of an establishment".[21] A case-by-case analysis is hence necessary in order to verify whether there is an inextricable link between the activities of an EU establishment and the data processing activities of a non-EU controller or processor. If such a link is identified, "EU law will apply to that processing by the non-EU entity, whether or not the EU establishment plays a role in that processing of data".[22] Again, however, extensive interpretations can raise uncertainties: the "wide view of 'context' arguably risks rendering 'context' as a connecting factor meaningless" (Hon et al., 2013, p. 225), thus leading to legal uncertainties as to the applicability of the EU law.

To sum up, the uncertainties that have been highlighted under the Directive as for the establishment criterion are likely to be inherited by the Regulation that merely replicates the wording of the Directive without clarifying its key notions. Moreover, since Article 3 of the GDPR extends the applicability of the establishment criterion to processors,[23] the interpretative challenges raised by the notions of "establishment" and "in the context of the activities of an establishment" will be extended to processors.

3.2. Untangling the Targeting Criterion

By virtue of the targeting criterion, the GDPR applies to the processing of personal data of data subjects who are in the Union by a controller or processor not established in the Union, where the processing activities are related (1) to the offering of goods or services to such data subjects in the Union or (2) to the monitoring of their behaviour. The ultimate aim of this criterion is to avoid the circumvention of the law

[17] Ibid., para. 55.

[18] Ibid., para. 56 (italics mine).

[19] Ibid., para. 57.

[20] Ibid., para. 53.

[21] Guidelines 3/2018, 6. At the same time, however, the EDPB has stated that "the existence of an establishment within the meaning of the GDPR should not be interpreted too broadly to conclude that the existence of any presence in the EU with even the remotest links to the data processing activities of a non-EU entity will be sufficient to bring this processing within the scope of EU data protection law".

[22] Guidelines 3/2018, 7.

[23] For an analysis of the GDPR obligations that are triggered when data are processed in the context of a processor's establishment in the Union, see Guidelines 3/2018, 10-12.

by controllers (and processors) through the relocation of their establishment(s) outside the Union.

The focus on "data subjects who are in the Union" allows a generalised application of the EU data protection legislation to all people physically present in the Union, irrespective not only of their residency or nationality,[24] but also of the duration of their stay on the EU soil, so that people present in the EU merely on holiday will also benefit from the high standards of protection prescribed under the Regulation (Colonna, 2014, p. 214). Such a generalised application of the EU data protection legislation is certainly consistent with the EU conception of privacy as a fundamental right that should be enjoyed by everyone regardless of residency and nationality.

The focus on "data subjects who are in the Union" allows a generalised application of the EU data protection legislation to all people physically present in the Union, irrespective not only of their residency or nationality, but also of the duration of their stay on the EU soil.

3.2.1. Offering of goods or services

One crucial interpretative challenge that may arise when applying the targeting criterion derives from the notion of "offering of goods or services". Indeed, in the light of this wording, two situations may arise: (1) a company actively endeavours to win customers in the EU market but fails to do so; (2) a company wins customers in the EU market even though it does not actively endeavour to do so (Svantesson, 2015, p. 232).

With reference to the first situation, it is clear from the wording chosen by the EU co-legislators that the Regulation would apply. Article 3 of the GDPR does not in fact refer to the "supplying" of goods or services but merely to the "offering" of goods or services. On the other hand, the applicability of the GDPR to the second situation is less clear. The online market is, in fact, populated by many companies that act at a global level without specifically targeting individuals in specific regions. In these situations courts may face an all-or-nothing choice of concluding either that such companies target "every country in the world", including the EU, or "no countries at all" (Svantesson, 2015, p. 232).

The Regulation hence leaves an open question: is it sufficient that a non-EU company merely knows that its products may end up in the EU to trigger the EU data protection legislation? Recital 23 of the GDPR offers some guidance in answering this question where it provides that "[i]n order to determine whether such a controller or processor is offering goods or services to data subjects who are in the Union, it should be ascertained whether it is *apparent* that the controller or processor *envisages* offering services to data subjects in one or more Member States in the Union".[25] This Recital also mentions some factors that may make apparent the controller's intention to offer goods or services to data subjects in the Union, such as the use of a language or a currency that are used in the Union or the mentioning of customers or users in the Union.

In order to determine whether a specific activity falls under the scope of the GDPR, the EDPB has emphasized the importance of investigating whether the facts of the case in question provide sufficient evidence of the non-EU entity's intention to offer goods or services to data subjects in the Union.[26] The EDPB has also recalled that, as stated under Recital 23, the mere accessibility of the controller's or processor's website in the Union "is insufficient to ascertain such intention".[27] In the light of this, if a company *happens* to sell goods/services to individuals in the Union without taking specific steps to target the EU market (passive sales) it should be left immune

[24] Recital 14 GDPR: "The protection afforded by this Regulation should apply to natural persons, whatever their nationality or place of residence, in relation to the processing of their personal data". See also, Guidelines 3/2018, 13.

[25] Recital 23 GDPR (italics mine).

[26] Guidelines 3/2018, 14-17.

[27] Recital 23 GDPR. Guidelines 3/2018, 16.

from any legal responsibility under the GDPR.[28] Whether this approach will be followed in practice is, however, yet to be seen.

The adoption of some technical solutions may also prevent companies from being caught under an "unwanted" jurisdiction. Geolocation technologies can, for example, be implemented in order to make explicit whether customers of a certain area are targeted or not. Indeed, geolocation technologies allow companies to pinpoint users' geographical location in order to tailor the content or to restrict access to the content of a website depending on the user's specific location (Svantesson, 2004,). Nonetheless, margins of error in the determination of the exact location of individuals are probably inevitable, as are the attempts to circumvent geo-location technologies by individuals themselves, for example by means of anonymising techniques (Svantesson, 2013, pp. 187–194).

As a further interpretative challenge, no distinction is made between companies that *routinely* target the EU market and those that only *occasionally* do so, meaning that companies that only occasionally offer services or goods to data subjects in the Union may be subject to the administrative burdens prescribed under the Regulation.

3.2.2. Monitoring of Data Subject's Behaviour

The Regulation also applies to the processing of personal data carried out by a controller or a processor not established in the Union where the processing activities are related to the monitoring of the behaviour of data subjects who are in the Union.

Recital 24 of the GDPR helps interpret this criterion by stating that "[i]n order to determine whether a processing activity can be considered to monitor the behaviour of data subjects, it should be ascertained whether natural persons are *tracked on the internet* including potential subsequent use of personal data processing techniques which consist of profiling a natural person, particularly in order to take decisions concerning her or him or for analysing or predicting her or his personal preferences, behaviours and attitudes".[29]

The Regulation also applies to the processing of personal data carried out by a controller or a processor not established in the Union where the processing activities are related to the monitoring of the behaviour of data subjects who are in the Union.

The notion of "monitoring" provided under Recital 24 of the Regulation seems to include "all forms of tracking and profiling on the internet, including for purposes of behavioural advertising".[30] This entails that any social networks, search engines, and websites that *track* the surfing behaviour of their visitors by means of cookies, JavaScript, ad banners, and spyware would be caught under the scope the Regulation. The EDPB has suggested an even broader interpretation of the notion of "monitoring" in considering that not only online tracking but also other types of technologies (e.g., CCTV, wearable and other smart devices) should be taken into account.[31]

In what seems to be an attempt to narrow down the scope of the Regulation, the EDPB has also stressed that *not* "any online collection or analysis of personal data of individuals in the EU would automatically" trigger the applicability of the GDPR. Rather, the controller's purpose for collecting the data and any further behavioural analysis based

[28] The EDPB considers, among others, the case of a US citizen that, while travelling in the EU, downloads a US news app that is exclusively directed at the US market. According to the EDPB, the data processing activity carried out by the US company offering the app would not fall under the scope of the GDPR. Indeed, in the view of the EDPB, "the element of 'targeting' individuals in the EU" is not present in the proposed scenario. See, Guidelines 3/2018, example 9, 14.

[29] Recital 24 GDPR (italics mine).

[30] Article 29 Data Protection Working Party. (13 December 2016). *Guidelines on Data Protection Officers ('DPOs')*. WP 243, 8.

[31] Guidelines 3/2018, 17-18.

on those data should be considered.[32] The range of monitoring activities falling under the scope of the GDPR remains, however, extremely broad. This may lead to the consequence of "a possible universal application of EU law"[33] and it is hard to imagine that this was the original intention of the EU co-legislators, or at least a desirable result, considering the problems of conflicting laws and of enforceability that, as will be discussed below, may be caused by such a(n) (over) broad applicability of the EU legislation.

4. Consequences of the Unilateral Expansion of Jurisdiction

Cross-border activities need laws designed to cross traditional geographical borders. A flexible approach to territorial scope is therefore necessary in order to make legislation fit for the transnational processing operations of the fast-moving digital age (de Hert & Czerniawski, 2016, p. 239). Nonetheless, a broad unilateral expansion of the EU jurisdiction across borders may inevitably lead to conflicts of laws and enforceability problems.

> **A flexible approach to territorial scope is therefore necessary in order to make legislation fit for the transnational processing operations of the fast-moving digital age.**

Firstly, in the absence of mutual agreements, the extraterritorial application of the EU data protection legislation leads to the (potential) simultaneous application of conflicting legal rules to the same facts or actions – rules dictated by different States that are all interested in preserving their jurisdiction in the presence of (some) connecting factors. Processors and controllers outside the EU may hence be trapped in a network of conflicting rules all resting on different possible legitimate triggers (e.g., nationality, territoriality), which would put them in a confusing and excessively burdensome position (de Hert & Czerniawski, 2016, pp. 239–240). In this overwhelming framework, companies may just choose not to comply with the EU data protection legislation (especially in the light of the enforceability problems that will be discussed below) or may simply be *unaware* of their compliance duties considering the uncertainties that affect the key terms of Article 3 of the GDPR.

Interestingly, the problems that arise from possible conflicts of law have been acknowledged by the EU Parliament in the position it adopted at first reading on 12 March 2014. Unsurprisingly (and unrealistically), the solution proposed by the EU Parliament in case of conflicting compliance requirements is, simply, that EU law always prevails: "[i]n cases where controllers or processors are confronted with conflicting compliance requirements between the jurisdiction of the Union on the one hand, and that of a third country on the other, the Commission should ensure that Union law takes precedence at all times…".[34]

Secondly, problems of enforceability inevitably accompany the extraterritorial application of the Regulation. Investigations and enforcement actions related to activities conducted by foreign companies with no physical presence in the Union and with only a loose identifiable connection with the EU are bound to face several legal, administrative, and practical obstacles. Despite the broad extraterritorial claims made under the Regulation, the actual enforcement of its provisions is hence likely to be limited to the bigger actors that have a strong impact on the EU market (Svantesson, 2015, p. 232).

[32] Ibid., 18.

[33] The Article 29 Working Party first expressed its concerns about the "undesirable consequences" of "a possible universal application of EU law" with reference to the equipment criterion (WP-179, 31). However, the same concerns can now be extended to the newly adopted targeting criterion.

[34] Recital 90, Position of the European Parliament adopted at first reading on 12 March 2014 with a view to the adoption of Regulation (EU) No …/2014 of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation) (EP-PE_TC1-COD(2012)0011). (12 March 2014). Retrieved from: http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//NONSGML+TC+P7-TC1-COD-2012-0011+0+DOC+PDF+V0//EN.

In this regard, some have noted that similar enforceability problems are outweighed by the *symbolic* value of extraterritorial claims. Indeed, assuming that companies generally prefer not to engage in activities that may turn out illegal, extraterritorial claims have an important deterrent effect for foreign companies (Svantesson, 2015, p. 233). This is what has been labelled "bark jurisdiction", i.e. "jurisdictional claims … that have virtually no prospect of being exercised in reality", as opposed to "bite jurisdiction" (Svantesson, 2014, pp. 58–59). Despite its weak binding force, bark jurisdiction allows States to signal to the international community their attempts to grant an effective protection of the right to privacy and hence to assert the international legitimacy of such attempts (Svantesson, 2014, p. 60; 2015, p. 233).

However, I agree with the statement that "the jurisdictional claims made under Article 3 of the … Regulation (as well as in Article 4 of the … Directive) are too wide, and some of the substantive rules (eg the requirement of a data protection officer) too burdensome to be viewed as legitimate bark jurisdiction" (Svantesson, 2015, p. 233). After all, "[t]he applicability of law to conduct, or the adjudication of a dispute by a court or regulator, is not a purely theoretical matter, but must have a reasonable chance of enforcement in order to have meaning" (Kuner, 2010, p. 236). Meaningless forms of jurisdiction may instead undermine the general respect for data protection law (Kuner, 2007, p. 125). A noted by Reed, enforcement is an essential component of the legitimacy of a governance system: "[a] regulator which is … accepted as having legitimate authority can easily lose that authority if it has no effective way of enforcing its rules. Conversely, a regulator which achieves a high level of compliance will enhance its legitimacy" (2013, p. 374).

5. Conclusion

A flexible approach to the territorial scope of the EU data protection legislation is necessary in order to address the increasingly transnational data processing activities that feed the modern digital age. Nonetheless, as seen above, flexibility often comes at the expense of clarity. Under the establishment criterion, the Regulation is likely to perpetuate the uncertainties that have emerged under the Directive with reference to the notions of "establishment" and "in the context of the activities of an establishment". The concept of "offering of goods or services" would also benefit from clarifications considering the practical difficulties that may emerge when confronted with the real-word situations of the online market, while the notion of "monitoring" data subjects' behaviour may lead to the "undesirable" consequence of a "possible universal application of EU data protection law".[35] Conflicts of laws and enforceability problems are hence likely to emerge in a similar (confusing) framework where the boundaries of the EU jurisdiction applicability have been unilaterally stretched by the EU co-legislators. As a result, in the absence of a mutual agreement whereby States agree on which law should apply in which situation, the very objective of the EU data protection legislation may be undermined: *effective* protection of fundamental rights in general, and right to privacy in particular. ■

[35] WP 179, 31.

About the author:

Isabella Oldani

Isabella Oldani is a PhD candidate at the School of International Studies of the University of Trento (Italy). Her research mainly focuses on data protection issues in relation to EU data export restrictions. During her PhD, she has been visiting as a research student at the Centre for Commercial Law Studies of the Queen Mary University of London where she had the chance to work alongside the Cloud Legal Project. She is also admitted to the Italian Bar.

References

Article 29 Data Protection Working Party. (13 December 2016). *Guidelines on Data Protection Officers ('DPOs')*. WP-243.

Article 29 Data Protection Working Party. (16 December 2010). *Opinion 8/2010 on applicable Law*. WP-179.

Colonna, L. (2014). Article 4 of the EU Data Protection Directive and the irrelevance of the EU–US Safe Harbor Program? *International Data Privacy Law*, *4*(3), 203–221. https://doi.org/10.1093/idpl/ipu005.

de Hert, P., & Czerniawski, M. (2016). Expanding the European data protection scope beyond territory: Article 3 of the General Data Protection Regulation in its wider context. *International Data Privacy Law*, *6*(3), 230–243. https://doi.org/10.1093/idpl/ipw008.

European Data Protection Board. (16 November 2018). *Guidelines 3/2018 on the territorial scope of the GDPR (Article 3)* – Version for public consultation.

Hon, W. K., Hörnle, J., & Millard, C. (2013). Which Law(s) Apply to Personal Data in Clouds? In C. Millard (Ed.), *Cloud Computing Law* (pp. 220–249). Oxford: Oxford University Press.

Judgment of 1 October 2015, *Weltimmo*, C-230/14, ECLI:EU:C:2015:639.

Judgment of 13 May 2014, *Google Spain and Google*, C-131/12, ECLI:EU:C:2014:317.

Kuner, C. (2003). *European Data Privacy Law and Online Business*. New York; Oxford: Oxford University Press.

Kuner, C. (2007). *European Data Protection Law: Corporate Compliance and Regulation* (2nd ed.). New York; Oxford: Oxford University Press.

Kuner, C. (2010). Data Protection Law and International Jurisdiction on the Internet (Part 2). *International Journal of Law and Information Technology*, *18*(3), 227–247. https://doi.org/10.1093/ijlit/eaq004.

Position of the European Parliament adopted at first reading on 12 March 2014 with a view to the adoption of Regulation (EU) No .../2014 of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation) (EP-PE_TC1-COD(2012)0011). (12 March 2014). Retrieved from: http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//NONSGML+TC+P7-TC1-COD-2012-0011+0+DOC+PDF+V0//EN.

Reed, C. (2013). Cloud Governance: The Way Forward. In C. Millard (Ed.), *Cloud Computing Law* (pp. 362–389). Oxford: Oxford University Press.

Report of the International Law Commission, Fifty-eighth session. (1 May–9 June and 3 July–11 August 2006). UN Doc. A/61/10, Annex E, para. 2. Retrieved from: http://legal.un.org/ilc/documentation/english/reports/a_61_10.pdf

Sachdeva, A. M. (2007). International Jurisdiction in Cyberspace: A Comparative Perspective. *Computer and Telecommunications Law Review*, *13*(8), 245–258.

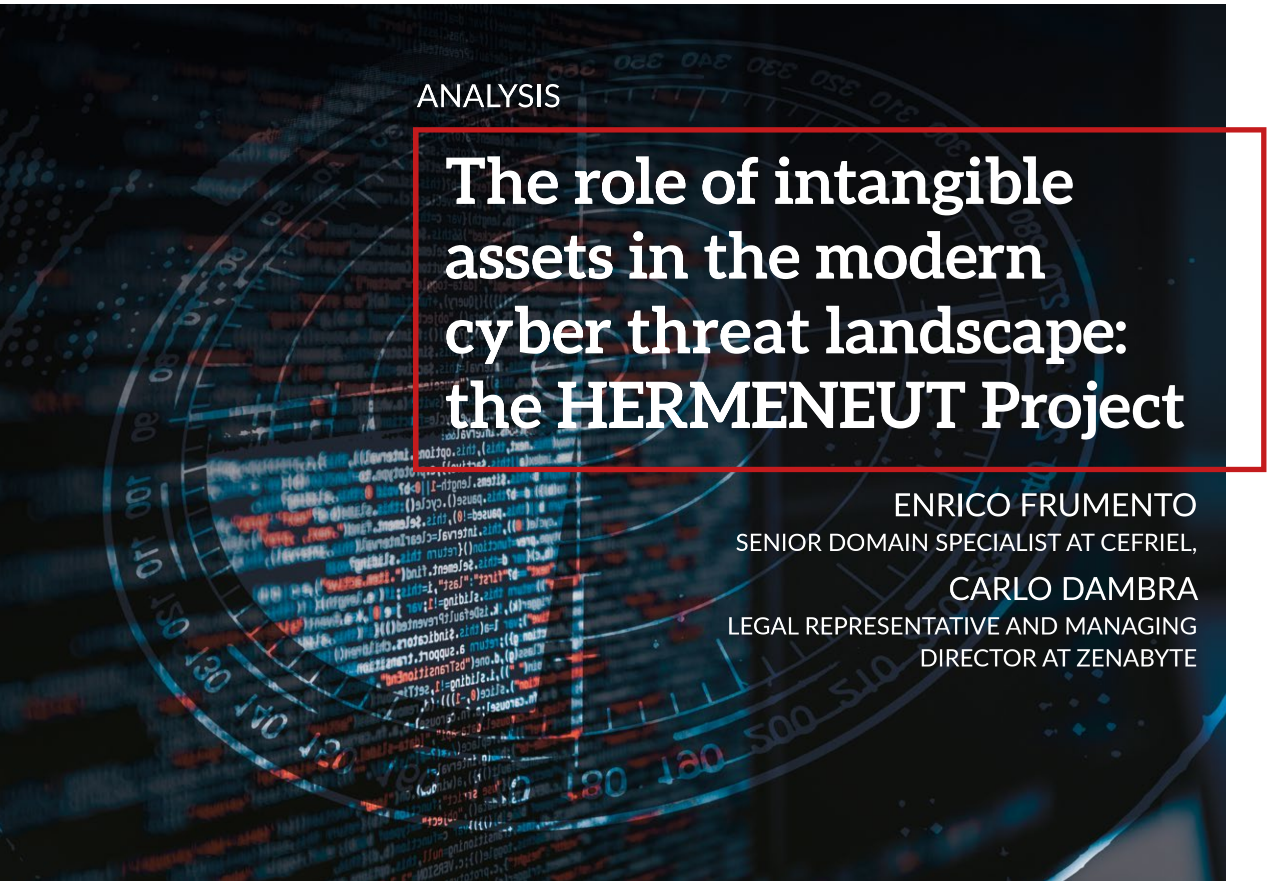
Senz, D., & Charlesworth, H. (2001). Building Blocks: Australia's Response to Foreign Extraterritorial Legislation. *Melbourne Journal of International Law*, *2*(1), 69–121.

Svantesson, D. J. B. (2004). Geo-Location Technologies and Other Means of Placing Borders on the 'Borderless' Internet. *The John Marshall Journal of Computer and Information Law*, *23*(1), 101–139.

Svantesson, D. J. B. (2013). *Extraterritoriality in Data Privacy Law*. Copenhagen: Ex Tuto Publishing.

Svantesson, D. J. B. (2014). The Extraterritoriality of EU Data Privacy Law: Its Theoretical Justification and Its Practical Effect on U.S. Businesses. *Stanford Journal of International Law*, *50*(1), 53–102.

Svantesson, D. J. B. (2015). Extraterritoriality and targeting in EU data privacy law: the weak spot undermining the regulation. *International Data Privacy Law*, *5*(4), 226–234. https://doi.org/10.1093/idpl/ipv024.



ANALYSIS

The role of intangible assets in the modern cyber threat landscape: the HERMENEUT Project

ENRICO FRUMENTO
SENIOR DOMAIN SPECIALIST AT CEFRIEL,

CARLO DAMBRA
LEGAL REPRESENTATIVE AND MANAGING DIRECTOR AT ZENABYTE

Introduction

Today, the elusiveness of Targeted Attacks (TA)[1] and the number of evasion tactics exploited by the ongoing attacks is so large that monolithic defence strategies are no longer efficient. Successful attacks are built to stay under the detection threshold on all security layers (from network to the human layer): e.g. network scanning is usually today a tenuous activity, systems' compromising happens with tailored copies of unique malware, and phishing campaigns are tailored around single humans (DOGANA, 2018). Cybercrime is increasingly going in the direction of sophisticated "low-and-slow" attacks (Johnson, 2016). The low-and-slow approach involves attackers remaining invisible for as long as possible, while stealthily moving from one compromised host to the next without generating regular or predictable network traffic patterns or data exfiltration instances as they hunt for specific data or system targets. The rapidity of single attack steps is one crucial element of being stealthy. The defence paradigms must therefore adapt to this increasingly flexible and non-noticeable scenario, where the usual defence systems based on pattern recognition are not effective anymore. The endpoints receive the new pattern signatures and heuristics after the identification and isolation of a new virus. Novel ad-hoc malware is adopting low-and-slow 1:1 infection schemes (see the discussions on malware 2.0 in Frumento, Lucchiari, and

[1] An attack can be considered a targeted attack (Trend Micro Inc, 2015) when it fulfils three main criteria: 1) the attackers have a specific target in mind and are shown to have spent considerable time, resources and effort in setting up or carrying out the targeted attack; 2) the main aim of the targeted attack is to infiltrate the target's network and steal information from their servers; 3) the attack is persistent, with the attackers expending considerable effort to ensure the attack continues beyond the initial network penetration and infiltration of data.

Pravettoni, 2010). As a result, a recent report from FireEye cites that “the average time from an email phishing breach to detection is 146 days globally, and a colossal 469 days for the EMEA region” (FireEye, 2017).

The low-and-slow approach involves attackers remaining invisible for as long as possible, while stealthily moving from one compromised host to the next without generating regular or predictable network traffic patterns or data exfiltration instances as they hunt for specific data or system targets.

The early detection of the weak signals of an ongoing attack is one important challenge in today’s security market. One promising approach to this challenge is the adoption of Artificial Intelligence (AI) to analyse the data with the objective to capture emerging and unnoticed patterns/trends. In addition, Cyber Threat Intelligence (CTI) tools are facing this challenge. However, in this second case, the most problematic issue is not the complexity of the evaluation models but the potentially uncontrollable divergence of their forecasts. CTIs predictive power is tied to the preciseness of the Indicator of Compromise (IoC), whose collection is regulated through different bodies (mainly, in the EU, such as the ISACs (ENISA, 2018) or crowd-based efforts such as VERIS CDB (VERIS, 2018) and supporting (usually de-facto) technologies (STIX being the reference serialisation language (STIX, 2018). What limits CTIs is therefore the instability of their forecast models, which require efforts to collect IoCs, elaborate, and distribute the early alerts. These limitations go beyond the possibilities of an organisation with low-budget security programs.

The early detection of the weak signals of an ongoing attack is one important challenge in today’s security market.

For the above reasons, the EU set up a significant effort to keep secure and coherent information-sharing and to feed the forecast models with correct data. The achievement of this objective happens through legal reporting obligations (see the GDPR) and organisations at national or EU levels (Computer Emergency Response Team or CERT, Computer Security Incident Response Team or CSIRT and sectorial Information Sharing and Analysis Center – ISAC). However, this mechanism is not still wholly deployed; for a company with low-budget security program, the costs and technical/organisational efforts to fully integrate into the EU cybercrime forecast infrastructure are still relatively high (also in terms of required competencies). HERMENEUT’s aim is to bridge the gap for organisations with low-budget security programs, creating an “agile” service, yet with some approximations, immediately exploitable to get insights and criteria for the cyber risk mitigation. On the other hand, the described infrastructure and IoCs are covering almost only tangible/technical indicators of an ongoing cyberattack. The world of intangibles is still mainly not covered (e.g. only data leaked are) by the EU information collection infrastructure and forecast models.

Context

As reported by Ahmed (2017), the current approaches to IT security and risk management tend to underestimate the following key aspects:

- The human factor (covering subjective, organisational, societal, and economic aspects) in the identification of vulnerabilities to cyberattacks. This aspect is often ignored despite the fact that, as recently demonstrated (DOGANA, 2018), Social Engineering 2.0 (SE) attacks generate the highest costs in terms of both consequences of and protection against attacks (ENISA, 2017) and that SE attacks such as phishing are ten times more common in social media posts than malware. Moreover, the ease of creating fraudulent social media accounts for known brands drives a clear preference for phishing in social media-based attacks, though other types of media are also abused for the same purpose.

- The strategy of the attacker in the identification of vulnerabilities and assets at risk: modern attacks follow the same business logic as that followed by big companies that involves multidisciplinary competences in the definition process of their strategies and business plans (Thomas, et al., 2015; ENISA, 2017). The same multidisciplinary approach combining engineering, Risk Assessment (RA), economic, cognitive, behavioural, societal, and legal knowledge is needed to properly address the strategy of professional IT attackers.
- The role of intangible assets in the quantification of the cyberattack consequences; as reported in Kerber & Jessop (2015): "More than half the value of companies worldwide is in intangible assets, such as intellectual property, much of which is stored on computers and could therefore be vulnerable to hackers. That figure could be as high as $37.5 trillion of the $71 trillion in enterprise value of 58,000 companies, according to Brand Finance, a consultancy specializing in valuation of intangible assets." Moreover, according to statistics (PAYCHEX, 2016), more than 70% of attacks target small businesses and as much as 60% of hacked small and medium-sized businesses go out of business after six months.

The current approaches to IT security and risk management tend to underestimate the following key aspects: the human factor, the strategy of the attacker, and the role of intangible assets.

Several sources report that estimates of cybercrime costs are not accurate enough. For example, ENISA: "the measurement of the real impact of incidents in terms of the costs needed for full recovery proved to be quite a challenging task". Analysing the past cyberattacks and the various white papers recently published by various organisations (Deloitte LLP, 2016; Ponemon, 2018; Zurich Insurance Company Ltd, 2014) makes it possible to observe that a successful cyberattack may lead to several consequences for the victim organisation:

- Direct consequences: the (partial or entire) loss or compromise or damage of one or more tangible or intangible assets as a direct effect of the cyberattack.
- Indirect consequences: the direct consequences of the attack may generate, as a cascade effect, other losses in the tangible or intangible assets of the organisation (e.g. a theft of personal data from a credit card company may generate a loss of reputation and as a further consequence a loss of clients).
- Attack-related costs: beside the direct and indirect consequences, being victim of a cyberattack generates other costs, including those reported in Table 1.

Table 1. Attack related costs

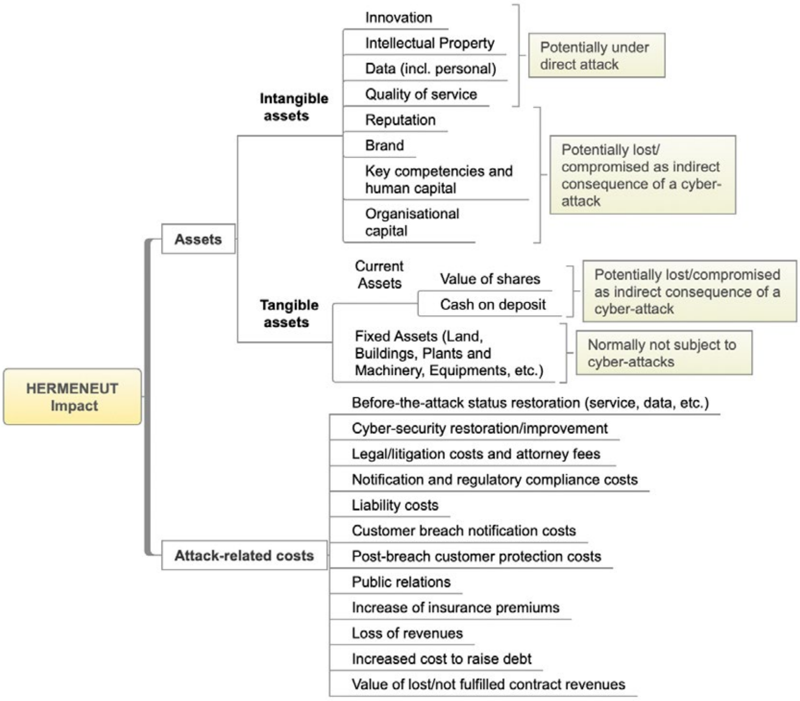
Before-the-attack status restoration (service, data, etc.)	Cybersecurity restoration/improvement
Legal/litigation costs and attorney fees	Notification and regulatory compliance costs
Liability costs	Customer breach notification costs
Post-breach customer protection/care costs	Lost customers recovery
Public relations	Increase of insurance premiums
Loss of revenues	Increased cost to repay debt
Value of lost/not fulfilled contract revenues	

The impact tree with tangible and intangible assets together and the possible attack-related costs is shown in Figure 1.

a. The role of intangibles in current attacks

As mentioned in the previous sections, the role of intangible assets is an often-neglected element for the quantification of the cyberattack consequences. The consequences of data breaches in terms of impact on tangible and intangible assets are a problem that has been studied for several years (Riddle, et al., 2011). Cyberattacks can damage physical – tangible – assets of the victimised institutions (e.g., turbines destroyed due to the manipulation of their control systems (Langner, 2013). More frequently, though, the damage will not be physical. Increasingly, the attacks are hitting intangible assets as a primary target – e.g. automated cyber *crowdturfing*[2] attacks (Yao, et al., 2017) – or as a consequence of the attack's main goal – e.g. Uber data breach in 2017).

Fig. 1. HERMENEUT impact tree


HERMENEUT Impact
Assets
Intangible assets
Innovation
Intellectual Property
Data (incl. personal)
Quality of service
Reputation
Brand
Key competencies and human capital
Organisational capital
Potentially under direct attack
Potentially lost/ compromised as indirect consequence of a cyber-attack
Tangible assets
Current Assets
Value of shares
Cash on deposit
Potentially lost/compromised as indirect consequence of a cyber-attack
Fixed Assets (Land, Buildings, Plants and Machinery, Equipments, etc.)
Normally not subject to cyber-attacks
Attack-related costs
Before-the-attack status restoration (service, data, etc.)
Cyber-security restoration/improvement
Legal/litigation costs and attorney fees
Notification and regulatory compliance costs
Liability costs
Customer breach notification costs
Post-breach customer protection costs
Public relations
Increase of insurance premiums
Loss of revenues
Increased cost to raise debt
Value of lost/not fulfilled contract revenues

Modelling these attacks is difficult for the relative "obscurity" of the cybercriminal attack plan. Intangible assets (i.e. reputation, trust in the organization, patents, trademarks, knowledge, expertise, human-capital, etc.) are now recognised as critical to the performance of companies and nations. At the macroeconomic level, many studies stress the dominant nature of intangible investment as well as its important contribution to economic growth and productivity (Nakamura, 2003). At the microeconomic level, besides research which focuses on specific intangibles such as R&D, patents, or brands, studies also stress the importance of intangible assets for corporate performance, using a comprehensive approach (Ahmed, 2003). Intangibles often contribute up to 80% of an organisation's value.

[2] Crowdturfing is a combination of "crowdsourcing", meaning recruiting large numbers of people to contribute a small effort each toward a big task (like labelling photos), and "astroturfing", meaning false grassroots support (in the form of bogus reviews or comments, for example) (Jacobs, 2014).

Intangible assets (i.e. reputation, trust in the organization, patents, trademarks, knowledge, expertise, human-capital, etc.) are now recognised as critical to the performance of companies and nations. (...) Intangibles often contribute up to 80% of an organisation's value.

b. The HERMENEUT approach

Given the described scenario, the aim of HERMENEUT is to create an inclusive approach to cybersecurity cost-benefit analysis. It starts (i) from an integrated assessment of vulnerabilities and their likelihoods and, (ii) exploiting an innovative macro- and microeconomic model for intangible costs, ends (iii) with an estimation of the cyber-risks for an organisation or business sector followed by guidelines (iv) on investments, to mitigate the loss of an enterprise's integrity.

The HERMENEUT core model reported in Figure 2 represents the following fundamental steps:

1. Integrated estimation of the enterprise's vulnerability regarding both humans and technology.
2. Development of an economic cost model that quantifies the consequences of attacks for both attackers and victims.
3. Development of a full risk model for both tangible and, especially, intangible risks.
4. Mitigation measures for the loss of the enterprise's integrity, with particular emphasis on two business sectors (healthcare, intellectual property-intensive industries).
5. Development of a decision and policy-making tool supporting cost-benefit risk-based investments in cybersecurity mitigation (including cyber-insurance). The tool, leveraging on an open-source RA framework, integrates the models and the knowledge created in the project. It provides the users (i.e. decision-makers in cybersecurity cost-benefit analysis and protection measures) with novel functionalities for (i) the estimation of tangible and intangible costs generated by cyber threats and (ii) risk-based and cost-based analysis and assessment of proper countermeasures for protection.

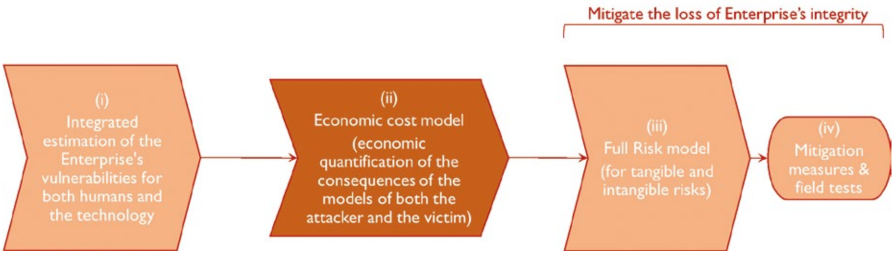
As defined in many standards (e.g. International Organization for Standardization, 2009), risk can be defined as the combination of **likelihood** of an event to occur and its **consequences.** When assessing the risk of cyberattacks for an organisation, the main difficulties are:

- Estimating the vulnerabilities of the organisation to cyberattacks and therefore the likelihood of being subject to these attacks and the tangible and intangible assets at risk, as a direct or indirect consequence of the attack. Since it is impossible to estimate the likelihood of a cyberattack against a specific organisation, it is necessary to assess the technical and social vulnerability of the organisation and indirectly compute the probability of the cyberattack.
- Quantifying the possible consequences of the attacks on the tangible and intangible assets at risk. It is of particular importance to take into consideration the role that intangible assets can play, since related costs, often neglected, can be as large as for tangibles or exceed these.
- Assessing the risks and taking decisions on the best-possible investments to mitigate the risks of cyberattacks.

Moving from the organisation level to the industrial sector level, it is crucial to define policies and recommendations for stakeholders to adapt to and protect from the continuously changing cyber-risks; having a clear idea – for each sector – of the most common vulnerabilities of and the potential consequences for the assets at risk.

Therefore, HERMENEUT is proposing an inclusive approach to cybersecurity, addressing the problem not only from the technical point of view, but also introducing societal, institutional, and economic perspectives as illustrated in the diagram in Figure 3. It represents the general HERMENEUT model and adds to what Figure 2 has already shown a detailed view of the phases from (i) to (iv).

Fig. 2. Logical high-level view of the HERMENEUT approach


Mitigate the loss of Enterprise's integrity
(i)
Integrated estimation of the Enterprise's vulnerabilities for both humans and the technology
(ii)
Economic cost model (economic quantification of the consequences of the models of both the attacker and the victim)
(iii)
Full Risk model (for tangible and intangible risks)
(iv)
Mitigation measures & field tests

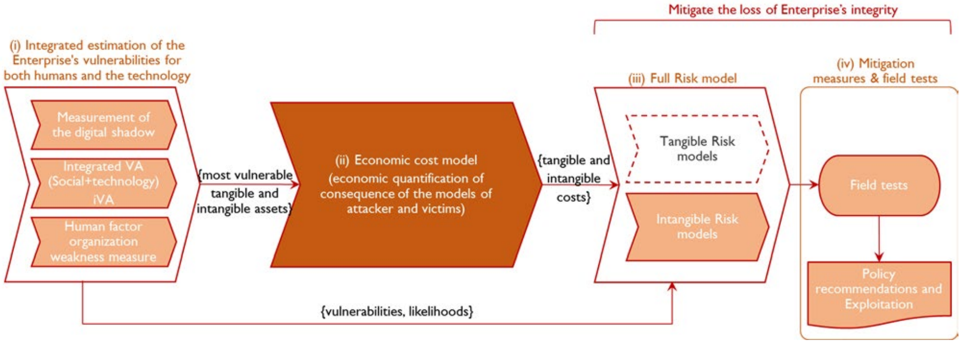
The role of the phase (i) is to detect the vulnerabilities and their likelihood, simulating the modern threat landscape through an integrated estimation of the enterprise's vulnerabilities, for both humans (through social engineering simulations and social-driven vulnerability assessment) and technology (e.g. simulating modern ad-hoc threats). This phase feeds the phase (ii), the HERMENEUT's economic cost model, and the phase (iii), the HERMENEUT's full risk model. The phase (iv) conjoins the results of the prior phases by deriving specific mitigation measures and field tests for the selected business sectors.

The inclusive HERMENEUT approach is based on:

- An integrated estimation of the enterprise's vulnerabilities for both the humans and the technology (phase (i) and the corresponding tangible and intangible assets at risk, considering the business plan of the attacker, the commoditisation level of the target organisation, the exposure of the target and finally the involved human factors and, on the same basis, estimating the likelihood of a potential cyberattack exploiting the assessed vulnerabilities. The resulting methodology is called integrated Vulnerability Assessment (iVA). This improved assessment considers the business plans of the attacker, the commoditisation level of the target organisations and its exposure, the relevant cognitive, psychological, and social factors.
- An innovative micro- and macroeconomic cost model focusing on intangible costs (phase (ii)), able to quantify the cost of the loss of one or more – especially intangible – assets at risk identified by the phase (i) based on an eclectic view of the role of intangibles by considering the impact of intangible factors and cyber-risk on organisation's sustainability at the microeconomic level and by considering the size of the GDP sensitive to cyber-risk at the macroeconomic level.
- A inclusive RA model (phase (iii) – taking as input the vulnerabilities and likelihoods of cyberattacks from the iVA and the economic quantification of potential consequences from the cost model – able to support decisions related to information security investments on hard (traditional) and soft mitigation measures (awareness and training campaigns, cyber-insurance, reorganisation of security procedures, etc.).
- Verification in two specific business sectors (healthcare and IP-intensive industry) of the developed models (phase (iv)).

To complete its actions, HERMENEUT uses a KISS (Keep It Simple and Stupid) approach, presenting perhaps less information but making the whole process easier to compile and less prone to inaccurate answers. This is supposed to avoid the problems of past methods based on long and complex questionnaires or profiling, where the quality of answers usually degrades along the compilation.

Fig. 3. The HERMENEUT concept

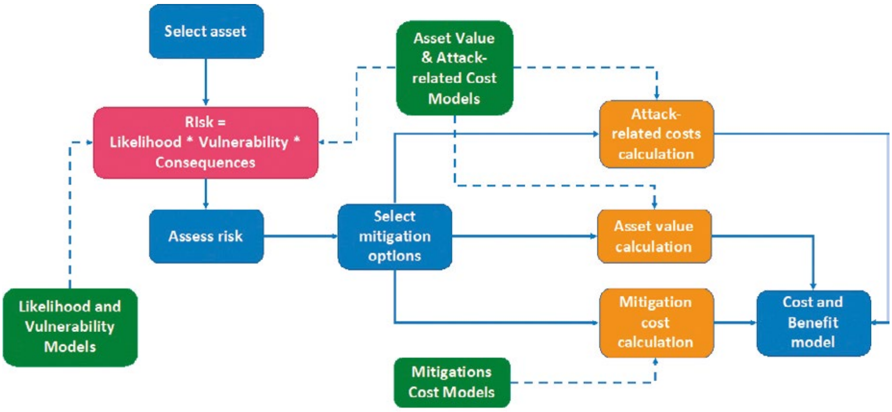

Mitigate the loss of Enterprise's integrity
(i) Integrated estimation of the Enterprise's vulnerabilities for both humans and the technology
Measurement of the digital shadow
Integrated VA (Social+technology) iVA
Human factor organization weakness measure
{most vulnerable tangible and intangible assets}
(ii) Economic cost model (economic quantification of consequence of the models of attacker and victims)
{tangible and intangible costs}
(iii) Full Risk model
Tangible Risk models
Intangible Risk models
(iv) Mitigation measures & field tests
Field tests
Policy recommendations and Exploitation
{vulnerabilities, likelihoods}

c. The assumptions of the model

HERMENEUT research statement has several commonalities with the CTI world but some approximations it uses differentiate it. HERMENEUT defines itself as a Strategic CTI, according to the classification reported in Chismon & Ruks (2015). As such, the main functionality offered by HERMENEUT is to present high-level information on changing risks to the CISO or the management board of an organisation. However, HERMENEUT is not a mitigation measure, but rather a decision support tool, which includes an integrated cyber-risk and economic model for the tangible and intangible asset losses. Although some of its elements come from the CTI world, the level and complexity of the model are very different. HERMENEUT's aim is to give a reasonable risk evaluation model for organisations with low-budget security programs, because of the approximations introduced. The intention of the project is to: 1) ease the adoption of a safer cyber posture and more predictive reactions without diminishing the quality of the forecast models; 2) ease the long-term inclusion of organisations in the EU CTI-based prevention model while managing the tangible and intangible assets in a unique conceptual framework. These assumptions lead to several optimisations:

- The collection of evidence and the positioning goes through questionnaires typically compiled by the CISO. This collection process poses limits and biases to the quality of the resulting data. The research hypothesis is that these approximations are not affecting the advantages of an immediately available solution for the estimation of the cyber risk.
- The inference engine is not using an AI but rather a deterministic algorithm (probability-based risk evaluation).

Fig. 4. The HERMENEUT RA approach


Select asset
Risk = Likelihood * Vulnerability * Consequences
Assess risk
Likelihood and Vulnerability Models
Asset Value & Attack-related Cost Models
Select mitigation options
Attack-related costs calculation
Asset value calculation
Mitigation cost calculation
Cost and Benefit model
Mitigations Cost Models

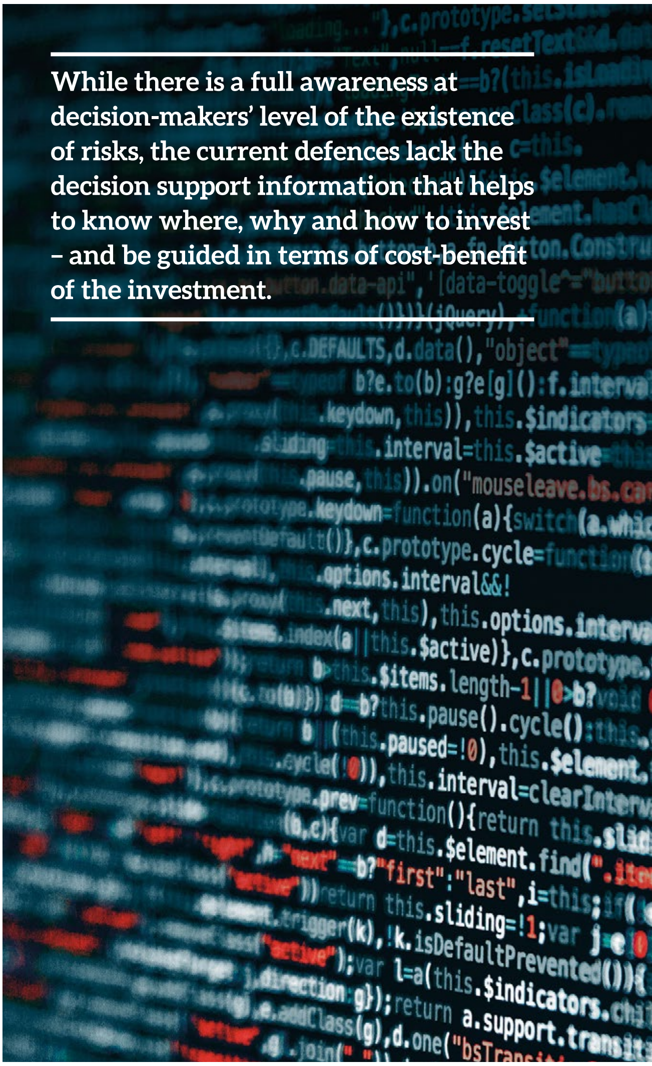
- HERMENEUT overcomes the limited update frequency of CAPEC (once a year) by proposing custom dynamic solutions for the proactive risk re-assessments and refinement models based on personal CISO knowledge and dark web data.
- The attack strategies described with STIX and defined by CAPEC have been simplified and grouped to be manageable by an average CISO, but also to not surpass the quality of the information collection tool used (i.e. questionnaires).

A confirmation of the expected usefulness of the HERMENEUT system comes from the recent data of a survey from SolidWorks (SolidWorks, 2018): “more than one-third of US organizations (37%) face security risks that exceed their overall security maturity. Within that group, 10% face a deficiency when it comes to protecting themselves from the threats in their environment”. A portion of the funnelling process of the HERMENEUT framework is about the assessment of the organisation’s maturity. Of the several maturity models currently in existence, the one used by HERMENEUT is simplified to rapidly offer an evaluation that organisations can make to benchmark their maturity. Cybersecurity leaders who complete the HERMENEUT online tool receive a report that scores the organisation’s risk and helps to shape future behaviours. However, the research questions of HERMENEUT are not preventing the future collaboration of HERMENEUT with the CTI community. The central hypothesis that the project wants to prove is the correctness of the assumptions made and their context of validity. The estimates reported above match the predictions of the economic and risk models, especially for the intangible assets.

d. 3-level HERMENEUT RA methodology

HERMENEUT RA is a three-phase funnel, where the goal of each level is to increase the confidence of the measure: each level also adds estimation of the connected costs. The three phases that follow the overall RA approach reported in Figure 4, are:

- **Level 1: Conservative (Screening) RA.** System vulnerability assessments are carried out using results of data collection and findings from the iVA, followed by risk evaluations using ranking techniques and then setting priority on remedial and preventive measures. Subsequent to this step, decisions regarding the prioritisation of resources can be initiated.
- **Level 2: Qualitative (secondary) RA.** The assets that require further consideration and have positive cost-benefit implications need additional data. These data allow for the reduction of uncertainty and more robust RA. Boston-square methods and specific vulnerability metrics are used alongside data elicitation from experts.



While there is a full awareness at decision-makers’ level of the existence of risks, the current defences lack the decision support information that helps to know where, why and how to invest – and be guided in terms of cost-benefit of the investment.

- **Level 3: Quantitative (Mainly Probabilistic) RA.** This will only be necessary for the most critical and complex assets. The level of detail depends on the uncertainty levels and models' requirements. At this level, assessment will involve a significant increase in the needed amount of asset- and company-specific data collection.

e. Future development

HERMENEUT will test the will test its assumptions in the healthcare and IP-intensive industries that are highly sensitive to TAs. This results from a combination of two factors: (i) these industries are often targeted by attackers and (ii) the results of an attack can create critical situations. At the same time, there is a grave imbalance between the effectiveness of recent attacks (e.g. the rising trend of the highly TAs), the evolution of the attacks purely meant to damage intangibles, and the relative inadequacy of current defences. While there is a full awareness at decision-makers' level of the existence of risks, the current defences lack the decision support information that helps to know where, why and how to invest – and be guided in terms of cost-benefit of the investment. The inclusive approach of HERMENEUT directly addresses this lack.

Acknowledgment

Funded under the EU Horizon 2020 HERMENEUT project, grant agreement No. 740322. ■

About the authors:

Carlo Dambra[1]

Dr. Carlo Dambra has been R&D Director of PROPRS Ltd. and is currently Legal Representative and Managing Director of ZenaByte s.r.l. He received his PhD in Computer Science and Electronic Engineering in 1993 from the University of Genova (Italy). He has a long-standing expertise in RTD project management on both nationally- and EC-funded projects (ICT, RTD Transport, RTD Environment). He is involved as researcher in the HERMENEUT (GA740322) and LETSCROWD (GA740866). He has been also invited as expert in RTD DG ICT and DG Research proposals evaluation and in support to negotiation.

Enrico Frumento[2]

Dr. Enrico Frumento works as a senior domain specialist at Cefriel (www.cefriel.com) in European and private-funded innovation projects on ICT Security. His research focuses on unconventional security, cybercrime and social engineering. He is the author of subject-related publications and books. He is the scientific coordinator of the project DOGANA (www.dogana-project.eu) which focuses on the contrast to the modern social engineering and the technical coordinator of the project HERMENEUT (www.hermeneut.eu), which focuses on developing an innovative methodology for the dynamic assessment of organization's vulnerabilities and corresponding tangible and intangible assets at risk.

[1] CEFRIEL Scarl, Politecnico di Milano, Viale Sarca 226, Milano, Italy, enrico.frumento@cefriel.com

[2] ZenaByte s.r.l., c/o DIBRIS, Via Opera Pia 11A, Genova, Italy, carlo.dambra@zenabyte.com

References

Abrams, L. (2016). *The shark Ransomware project allows you to create your own customized Ransomware.*

Ahmed, B. (2003). *The management of intangibles: The Organisation's most valuable assets.* London: Routledge.

Ahmed, B. (2017). *Micro - and macroeconomic modelling of intangible cyber-costs*.

Chismon, D. & Ruks, M. (2015). Threat Intelligence: Collecting, Analysing, Evaluating.

Deloitte LLP. (2016). *Beneath the surface of a cyberattack A deeper look at business impacts.*

ENISA. (2017). *Threat Landscape Report.*

ENISA. (2018). *Information Sharing and Analysis Centres (ISACs): Cooperative models.*

EU Patent Office and Office for Harmonization in the Internal Market. (2013). *Intellectual property rights intensive industries: contribution to economic performance and employment in the EU.*

FireEye, 2017. *Cyber Threats: A perfect storm about to hit Europe?.*

FRONTEX EU Agency for the Management of Operational Cooperation at the External Borders of the Member States of the EU, 2012. *CIRAM Common Integrated Risk Analysis Model*, Warsaw.

Frumento, E., Lucchiari, C. & Pravettoni, G. (2010). *Cognitive approach for social engineering*. Wien.

International Organization for Standardization. (2009). *ISO 31000 Risk management — Principles and guidelines.*

Jacobs, J. (2014). *Fake Followers for Hire, and How to Spot Them.*

Johnson, M. (2016). *Cyber crime, security and digital intelligence.* London: Routledge.

Kerber, R. & Jessop, S. (2015). *Asset Managers Urged to Make Cyber Risk Top Priority.*

Langner, R. (2013). *To kill a centrifuge. A technical analysis of what Stuxnet's creators tried to achieve the Langner group*. London: Routledge.

Nakamura, L. (2003). A Trillion Dollars a Year in Intangible Investment and the New Economy. In: *Intangible Assets*. Oxford: Oxford University Press.

PAYCHEX. (2016). *Creating a Cyber Security Culture in Your Business.*

Ponemon. (2018). *Cost of Data Breach Study.*

ProofPoint. (2018). *Protecting People Report. A quarterly analysis of highly targeted attacks.*

Riddle, B., Nyman, N. & Rees, J. (2011). *Estimating the costs of a data breach: An exercise at the new Hampshire state cancer registry.* Atlanta.

SolidWorks. (2018). *Secureworks Launches First Cybersecurity Maturity Model Based on an Organization's Inherent Risk.*

STIX. (2018). *A structured language for cyber threat Intelligence.*

Thomas, K. et al., 2015. *Framing Dependencies Introduced by Underground Commoditization*

Trend Micro. (2015). *Understanding targeted attacks. What is a targeted attack.*

VERIS. (2018). *Community Database.*

Yao, Y. et al. (2017). *Automated Crowdturfing Attacks and Defenses in Online Review Systems.*

Zurich Insurance Company Ltd. (2014). *The good, the bad and the careless. An overview of corporate cyber risk.*

OPINION

Creating a safer world of tomorrow

RENATA BILECKA
SENIOR TECHNOLOGY ENGAGEMENT MANAGER, SAMSUNG ELECTRONICS

These days, in the era of the Internet of Things, almost every device is connected to the World Wide Web. This is the future we are hurtling towards at breakneck speed. It is a vision equally full of promise and of security pitfalls. All the information gathered by our internet-enabled devices can help them anticipate our needs before we can even articulate them, but is it worth halting progress in the name of cybersecurity? And conversely: is it worth sacrificing some measure of safety, taking a risk to enable changes that could make our world a better, more accessible place? At Samsung, we ask ourselves these questions every day. Our response? We are taking up a series of initiatives that help secure data without compromising the development of devices that comprise what's next – the Intelligence of Things.

How devices communicate

These days, the smartphone functions as a remote control for the world around us. Certainly, the original functions of the cell phone, namely calling and texting, have been pushed aside in favour of the ability to access the Internet anywhere and anytime, including the advancing Internet of Things. This last one enables it to monitor and control various devices – the Things mentioned in the Internet of Things – remotely, wherever the user may be, thanks to specific apps dedicated to this exact purpose.

Also, on the rise are m-commerce and m-banking. The prefix "m-" means that these services, too, have already become smartphone-centric. According to conducted studies (Mobeedick, 2018), 31% of respondents shop online, and 22% of those finalise the payment on their mobile devices. 34% of respondents use mobile banking services. Furthermore, these devices are not only dedicated to personal use, but also to professional and business use. That means that there is a lot of sensitive data flowing through these mobile service hubs, including the data belonging to large companies and institutions.

These trends are not stopping; in fact, they are gaining momentum with every year. It has been estimated that by 2050, the IoT will contain more than 50 billion devices worldwide (McAfee, 2018). Even now, almost every person possesses at least one internet-enabled smart mobile device. By 2022, an average Pole is predicted to have around 3.9 web-enabled devices to their name (CISCO, n.d.).

Each one of those devices collects data about its users. It is what makes them work as well as they do – acquiring and processing data using intelligent systems. It allows the devices to optimise service and provide the users with what they need before they even ask, which is the core of effective human-intelligent machine interactions. A lot of the data used for that purpose is sensitive information, systematically obtained through everyday interactions.

By 2022, an average Pole is predicted to have around 3.9 web-enabled devices to their name (CISCO, n.d.).

"Sneaking things from the fridge" takes on a whole new meaning

Every one of these devices can now become the target of hackers; each of them contains potentially sensitive information about our habits, our needs, and our lives. If this data falls into the wrong hands, the fallout could be catastrophic for the user in question. And it would be unwise to forget that a smartphone or tablet can just as easily fall prey to a breach of security as any other device, be it a fridge, a washing machine, or any number of other devices linked up to the IoT.

Even today, the loss of a smartphone that has not been equipped with the appropriate security measures can have disastrous consequences. Certainly, most thieves are still motivated simply by the monetary worth of the device itself, yet there have already been situations where this was not the case (Ping-pong, 2018). Examples of sensitive data that can be acquired from a smartphone include credit and debit card information, personal information (dates of birth, addresses), potentially sensitive photographs, and various kinds of classified company data that could cause massive losses if revealed. According to Cisco's 2018 Annual Cybersecurity Report, more than 50% of cybersecurity breaches caused losses higher than USD 500,000, including loss of income, client, business opportunities, and costs of operation (Cisco, 2018, p. 46).

Be smart, be safe

It is no longer enough to simply lock your smartphone in a cupboard and hire a household security company. These devices, as all devices connected to the World Wide Web, are as vulnerable to a virtual break-in as a physical one. At the end of 2017, McAfee identified more than 20 million separate incidents of mobile-targeted malware. The losses associated with these programs just this year have been valued at 600 million dollars (McAfee, 2018).

To successfully counter these attacks, one must predict and remove potential exploits before the device leaves the design stage. One such solution is the Samsung Knox platform, by default built into every Samsung smartphone, tablet, and many different mobile devices in a way that is intrinsic to their design. The Knox platform has been built on various overlapping levels of security, which allows the creation of a secluded environment where all critical information is safely stored. Every user can manage multiple devices. Our belief as experts is that a secure ecosystem is the best way to ensure safety; securing each individual product might not be sufficient. That is why we design holistic solutions that protect entire systems and environments: it is critical to look beyond the device and think about solutions that integrate entire networks. And let's not forget that to complement security, users' education is a must – this is a crucial success factor for security systems.

And let's not forget that to complement security, users' education is a must – this is a crucial success factor for security systems.

Increasing productivity

Thankfully, as technology progresses, so do the systems used to keep it safe. The world is currently standing on the threshold of great changes. The security systems of the new age will be able to compute unstructured data and natural speech thanks to AI and machine learning. They will be constantly self-teaching, keeping several steps ahead of hackers and malware.

Will we be completely safe then? Well, that is uncertain. Every chain, after all, is as strong as its weakest link – which in this case is often the user.

The key to safety

Here at Samsung, we believe that the most important component for total information security is a bond of mutual trust, which once forged leads to openness and free exchange of information. Only by understanding our clients' habits and behaviours and the changing trends on the market will we be able to create effective data security systems. But to understand these habits and behaviours, we have to collect and analyse metadata about our users.

We need our partners to trust us.
And we want to earn that trust.

That is why we have isolated three elements that we believe are key to establishing our company as trustworthy: a team of experienced, knowledgeable experts, tried and true solutions, and total transparency in what we do with our partners' information. These points are the founding principles of the Samsung Security Management System (SSMS). As a result of these actions and open cooperation with our partners, last year alone we managed to isolate more than 4,800 potential security exploits in our open-source software.

This approach allows us to invest in the IoT without fear or compromise. We can offer our clients services that only yesterday seemed far-fetched even for science fiction. And we are certain that along with our cutting-edge solutions, we can offer the appropriate level of security – like a responsible and trustworthy partner should. ■

About the author:

Renata Bilecka
New Technologies Expert. 10+ years in the IT Advisory. Presents, teaches, negotiates, optimises, develops and digitally transforms customers' businesses through mobile and modern IT solutions. At Samsung Renata works on mobile & security solutions for B2B. Mom, traveller, and cyclist afterhours.

References

CISCO. (2018). *Cisco 2018 Annual Cybersecurity Report.* Retrieved from: https://www.cisco.com/c/dam/m/hu_hu/campaigns/security-hub/pdf/acr-2018.pdf

CISCO. (n.d.) *Cisco Visual Networking Index: Forecast and Trends, 2017-2022*. Retrieved from: https://www.cisco.com/c/en/us/solutions/collateral/service-provider/visual-networking-index-vni/white-paper-c11-741490.html

McAfee. (2018). *McAfee Mobile Threat Report Q1.* Retrieved from: https://www.mcafee.com/enterprise/en-us/assets/reports/rp-mobile-threat-report-2018.pdf

Mobeedick. (2018). *Polska.Jest.Mobi.* Retrieved from: http://jestem.mobi/2018/04/raport-polska-jest-mobi-2018-do-pobrania/

Ping-pong z hakerami. (2018, October 22). *Business Insider Polska.* Retrieved from: https://businessinsider.com.pl/technologie/jak-skutecznie-dbac-o-swoje-dane/e8x0vfv

European Cybersecurity Journal

Strategic perspectives
on cybersecurity management
and public policies

Readers' profile

- European-level representatives, sectoral agencies of the European Union, International Organisations Representatives;
- National-level officials of the Euro-Atlantic alliance, Government and Regulatory Affairs Directors & Managers;
- National and Local Government Officials as well as diplomatic representatives;
- Law Enforcement & Intelligence Officers, Military & Defence Ministries Officials;
- Legal Professionals, Representatives for Governance, Audit, Risk, Compliance, Industry leaders and innovators, active investors;
- Opinion leaders, specialised media, academic experts.

Types of contribution:

- Policy review / analysis / opinion – a Partner's article or a series of articles on crucial issues related to cybersecurity;
- Interview with Partner's representative;
- Research outcomes and recommendations;
- Advertisement of a firm, product or an event (graphical);
- Promotional materials regarding a cybersecurity conference / event (invitation, advertisement – graphical).

Do you want to share your opinion on national or European policies regarding cybersecurity? Do you want to publish outcomes of your research? Do you want to advertise?

The European Cybersecurity Journal is the right place to do it!

Prices of contribution

	PRICE (EUR)
Written contribution *Analyses, Opinions, Policy Reviews, Interviews, Research Outcomes*	100 / 1 page
Graphic contribution *Advertisement*	200 / 1 page
Graphic contribution *Advertisement*	350 / centerfold (2 pages)
Graphic contribution *Promotional campaign of an event*	250 / 1 page
Written contribution *Promotional campaign of an event*	400 / centerfold (2 pages)

CONTACT US: editor@cybersecforum.eu

The Kosciuszko Institute is a Polish think-tank founded in 2000. As an independent and non-profit organization, it gives itself the mission to contribute to the social and economic development of Poland in the European Union and as a partner of the Euro-Atlantic Alliance.

The experts of the Institute regularly cooperate with national and international organizations in the process of policy-making and initiating public debate on strategic issues.

Among its various areas of research, the Kosciuszko Institute leads its flagship project in the field of cybersecurity, within which the CYBERSEC Forum is organized.

We invite you to follow our initiatives and get involved.

The Kosciuszko Institute

is the publisher of

European Cybersecurity Journal