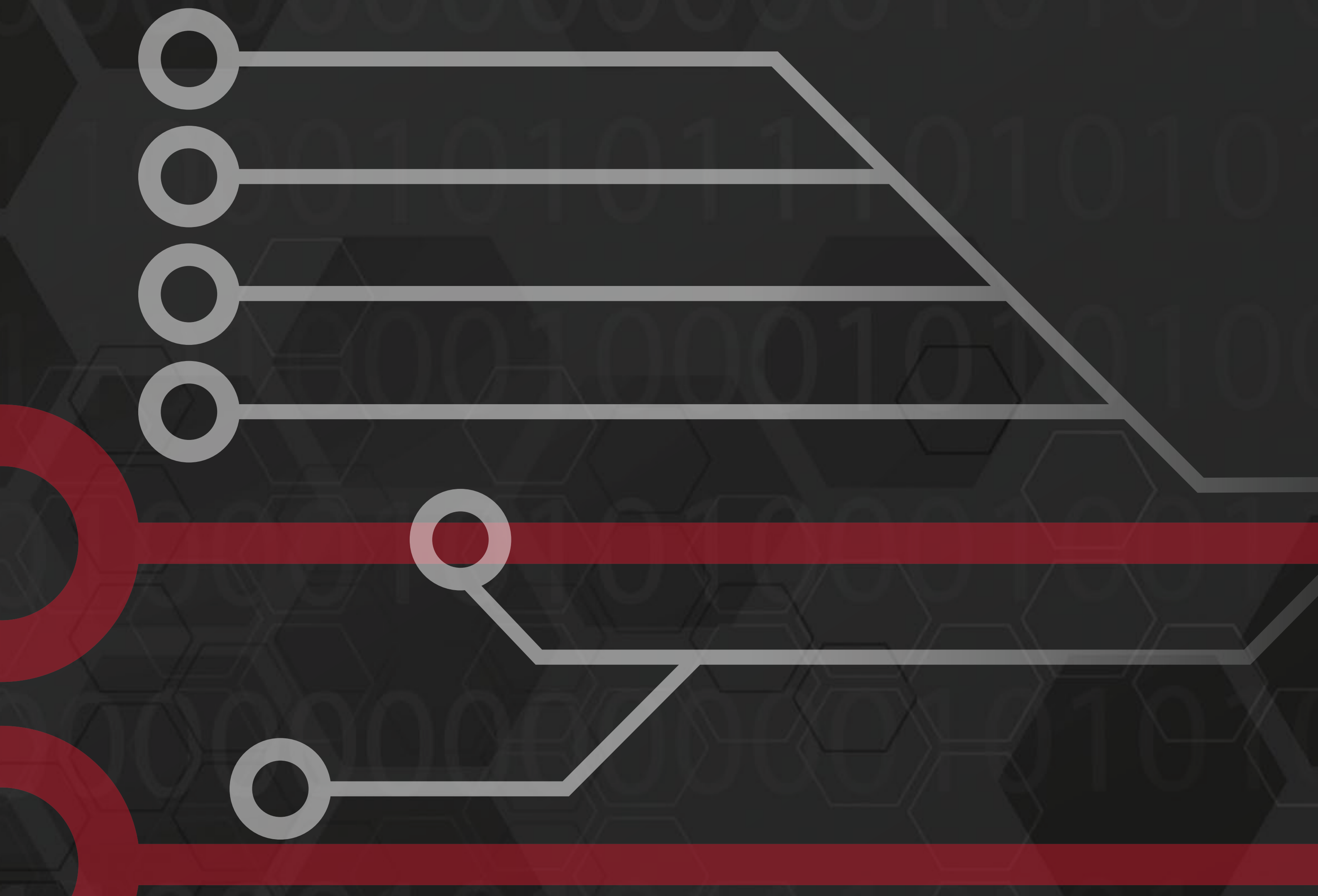
VOLUME 4 (2018) ▪ ISSUE 2

EUROPEAN CYBERSECURITY JOURNAL

STRATEGIC PERSPECTIVES ON CYBERSECURITY MANAGEMENT AND PUBLIC POLICIES



ANALYSES ▪ POLICY REVIEWS ▪ OPINIONS

THE KOSCIUSZKO INSTITUTE

EUROPEAN CYBERSECURITY JOURNAL

STRATEGIC PERSPECTIVES ON CYBERSECURITY MANAGEMENT AND PUBLIC POLICIES

The European Cybersecurity Journal is a new specialized quarterly publication devoted to cybersecurity. It will be a platform of regular dialogue on the most strategic aspects of 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

Designers: Paweł Walkowiak | perceptika.pl
Joanna Kaczor

Proofreading:
Justyna Kruk

ISSN: 2450-21113

The ECJ is a quarterly journal, published in January, April, July and October.

The Kosciuszko Institute

Citations: This journal should be cited as follows:
"European Cybersecurity Journal",
Volume 4 (2018), Issue 2, page reference

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

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

www.ik.org.pl
www.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.

EDITORIAL

BARBARA SZTOKFISZ
MARTA PRZYWAŁA
Research Fellows of the Kosciuszko Institute
CYBERSEC Project Managers
Chief Editors of the European Cybersecuirty Journal

Welcome to another issue of our European Cybersecurity Journal! This edition is brimming with must-read content for everyone who cares about the present and future state of cyberspace.

It is only halfway through, but the year 2018 has already proven that cybersecurity is a matter of global concern. The entry into force of the GDPR regulation and the NIS directive has increased social awareness about the impact that cyberspace has on every citizen. Also, the 2018 NATO Summit, during which global leaders discussed the most pressing challenges in the area of global security, demonstrated that cyber resilience is the biggest priority for the Allies. Together with the continuous adaptation of NATO's cyber capabilities, as part of NATO's long-term development, the Cyber Defense Pledge is supposed to reinforce the cyber defence and overall resilience of the Alliance. The process has already helped raise the awareness of the member countries about the need for a whole-of-society approach to cyber defence. Now, it is time to assess the specific actions taken by NATO members.

The present issue of ECJ starts off with an interview with Mady Delvaux-Stehres who touches upon the recent public policy activities and the most pressing opportunities and threats related to the further development of artificial intelligence.

The interview is followed by the article by Professor Harald Haas, Hamish Stewart, Harald Burchardt and Nikola Serafimovski who present LiFi, a technology that could be the answer to securing increasingly complex telecommunications networks which require an appropriate level of protection.

The article by Mauro Tortonesi reflects on IoT technologies in Smart City scenarios that are supposed to raise security issues in the near future.

In this issue, our readers will also find an in-depth analysis of the blockchain secure cloud which proposes to use blockchain algorithms for monitoring the execution of the security-aware task scheduling in the cloud.

Elsewhere, Adrian Neal presents his analysis of the crisis in the cybersecurity domain with concrete steps that need to be taken to counteract its further expansion.

Legal practitioners will welcome the article by Joost Bunk who writes about the intellectual property rights from the perspective of international humanitarian law.

Finally, this issue presents Japan's capabilities and potential to emerge as a new Asian cyber power.

We believe that the articles will be an important source of inspiration and incentive for cybersecurity stakeholders and decision-makers to contribute to the further exploration of these topics.

Enjoy your read and broaden your horizons!

Barbara Sztokfisz Marta Przywała

CONTENTS

POLICY REVIEW

2018 BRUSSELS NATO SUMMIT AND CYBER

MARTA PRZYWAŁA

is Research Fellow in the Kosciuszko Institute and CYBERSEC Project Manager. Her main areas of expertise are cybersecurity, as well as international security and defence. She graduated in French language and literature at the Jagiellonian University in Krakow. She holds double MA degree from the Centre for European Studies of the JU and Institut d'études politiques of the University of Strasbourg. She was granted the French government fellowship.

CDR WIESŁAW GOŹDZIEWICZ

is Legal Adviser at NATO Joint Force Training Centre in Bydgoszcz and Expert of the Kosciuszko Institute. He provides legal advice and training on the practicalities of the application of international humanitarian law and legal aspects of military operations. He served at the Public International Law Division of the Legal Department of the Ministry of National Defence. Commander Goździewicz (Polish Navy) joined the Armed Forces as a junior legal officer at the 43rd Naval Airbase in Gdynia. He is a graduate of the Faculty of Law and Administration of the University of Gdańsk.

Nowadays, when NATO faces approximately 5,000 cyber incidents per day, when cyber operations have become one of the main components of hybrid threats used of not only for the purposes of information campaigns or spreading propaganda, when transnational terrorist organisations resort to cyber means and methods to pursue their sinister goals, when destructive potential of cyber tools is not a secret anymore, it comes as no surprise that cyber threats remain high on the agenda of not only NATO, but also the whole international community. Therefore, the Alliance has to remain flexible and agile, become proactive rather than reactive in countering those threats, continue and enhance cooperation with key stakeholders: nations (both members and partners), international organisations, in particular the UN and the EU, but also the OSCE and the Council of Europe (note the Budapest Convention), and the private sector. Outdated or obsolete policies should be amended or revoked without delay, and developments across the whole DOTMLPFI[1] spectrum accelerated to the maximum extent possible.

[1] Any combination of Doctrine, Organisation, Training, Materiel, Leadership, Personnel, Facilities and Interoperability.

During the 2014 Wales NATO Summit, Allies recognised that international law (including Law of Armed Conflict) applies in cyberspace, and that the impact of cyberattacks could be as harmful to our societies as a conventional attack and trigger a response under Article 5 of the North Atlantic Treaty. As a result, cyber defence was recognised a part of NATO's core task of collective defence.

What does it mean?

It is now possible to collectively respond to an attack in cyberspace, and it is not different from a conventional attack conducted at sea, in the air or on the land. Evoking Article 5 and NATO's response depends on a political decision – or a judgement call – made by the North Atlantic Council by consensus. What is important, the response does not have to be symmetric or in-kind. NATO's mandate is purely defensive, thus the Alliance does not develop any offensive cyber capabilities, just as it does not develop offensive 'conventional' capabilities. Similarly, the Alliance does not own any equipment or means either (except for the NATO Airborne Early Warning and Control Component). In this regard, it relies on its member states and their armed forces operating in the joint structures. Therefore, it is a national prerogative of the member nations to develop and possess certain defence capabilities, as stated in Article 3 of the North Atlantic Treaty. Those capabilities need to be made available to NATO at its request, as it has always been. This includes providing NATO voluntarily with these national assets in need.

An alliance of shared values and transatlantic unity was one of the topics during the 2018 Brussels NATO Summit.

The Summit should endorse the decisions made during the November 2017 Defence Ministerial, particularly the decision to integrate voluntarily contributed national cyber capabilities (including offensive ones) in support of allied operations.

The unit which, among others, will be responsible for operational control over these voluntarily contributed cyber means is the Cyber Operations Centre (CyOC) within Supreme Headquarters Allied Powers Europe (SHAPE) and respective cells in the Joint Force Commands (JFCs). Its creation was approved by Allies during the November 2017 Defence Ministerial. Being 'eyes and ears' of the respective commanders in cyberspace, the CyOC is supposed to enhance situational awareness in cyberspace and help integrate cyber into NATO's planning and operations at all levels. It will not be a cyber command centre as there will not be any supranational command. While the CyOC is to operate within the existing NATO frameworks, its main aim is to equip the Supreme Allied Commander Europe (SACEUR) with all the necessary tools to operate in cyberspace. What still needs to be agreed upon is an overall increase in NATO Command Structure personnel and a greater emphasis on the regional focus of the commands.

Allies should also agree to review NATO's cyber-related policies, including the issue of how NATO should collectively respond to cyberattacks.

The *Cyber as a Domain Implementation Roadmap* identifies 10 Lines of Effort (LoEs). From an operational perspective, the most important ones are the integration of cyber effects and the cyber doctrine development as they are closely related to each other. NATO needs to accelerate the implementation of its Doctrine on Cyberspace Operations to enable cyber operations to be conducted in line with legal, political and military guidelines and principles. Until then, NATO's ability to operate in and through cyberspace, defend in cyberspace equally efficiently as on the land, in the air or at sea, while at the same time acting within the boundaries of international law and in line with the principles of responsible behaviour, will remain limited.

At the 2014 Wales NATO Summit, Allies reaffirmed their commitment to spend a minimum of two percent of each Ally's GDP on defence.

Moreover, the Cyber Defence Pledge from the 2016 Warsaw NATO Summit commits Allies to allocate adequate resources nationally to strengthen their cyber defence capabilities, even if there is no specified minimum amount.

Fairer burden-sharing was one of the most important topics during the Brussels NATO Summit.

And it will not leave the table as long as the U.S. continues to contribute the most to NATO's total military spending. According to estimates from 2017, only six members fulfilled the two percent requirement[2], with only eight countries estimated to do so in 2018. However, even with eight NATO Allies hitting the target, it leaves 21 behind. The situation will become more dramatic for Allies in the European Union after Brexit as the contributions of non-EU NATO countries (the U.S., the UK, Turkey, Canada and Norway) will account for staggering 80 percent or so of the total budget.

> ***During the Summit, the progress in defence expenditures that has been achieved in recent years should be acknowledged; therefore, it should be also highlighted that this has not yet occurred across the whole of the Alliance.***

Defence expenditures shall be further increased, and national plans are needed to achieve commonly agreed goals as part of this commitment, including cyber goals. There is a need for European leaders who show political will and leadership to convince their electorates that Europe must do more for the military, so that credibility of Europe's defences is regained.

During the 2016 NATO Summit in Warsaw, Allies pledged to strengthen and enhance the cyber defences of national networks and infrastructures as a matter of priority.

What does it mean?

Resilience was the biggest priority for Allies during the 2018 Brussels NATO Summit

Together with the continuous adaptation of NATO's cyber defence capabilities, as part of NATO's long-term development, the Cyber Defence Pledge will reinforce the cyber defence and overall resilience of the Alliance. As NATO depends on national capabilities in nearly every area, its ability to operate in the cyber domain also hinges upon its success to set more ambitious capability targets for its member states and to encourage them to plug the identified gaps. By inducing Allies to perform more regular assessments of their levels of preparedness, the Cyber Defence Pledge should make this effort easier in the future.

Strengthening deterrence and defence was discussed during the 2018 Brussels NATO Summit.

> ***National development concerning the Cyber Defence Pledge engagements will be assessed for the first time with regard to the set criteria.***

Allies have carried out self-assessments of their cyber defence hygiene by reporting on seven capability areas: strategy, organisation, processes and procedures, threat intelligence, partnerships, capabilities, and investments. They were supposed to benchmark these assessments according to four levels ranging from advanced to a relative beginner. These assessments will allow NATO staff to develop more precise and relevant metrics, to form a more reliable common baseline of overall NATO capabilities, as well as to identify gaps and prioritise requirements. On this basis, the well-known NATO Defence Planning process, which has already incorporated a set of basic cyber capability targets for each NATO member state, will be able to suggest more ambitious targets that are better adapted to the needs of individual states in the future. The peer pressure that greater transparency should create will incentivise Allies to meet their assigned targets and to stimulate bilateral assistance. The process should also help identify best practices. The results will be published in a report available only to the heads and the governments of the member states.

Although the details will not be available to the public but shared only within and among the Summit participants, it is safe to assume that Poland will be among the leaders in the delivery of the Pledge. There is a number of arguments behind this assumption.

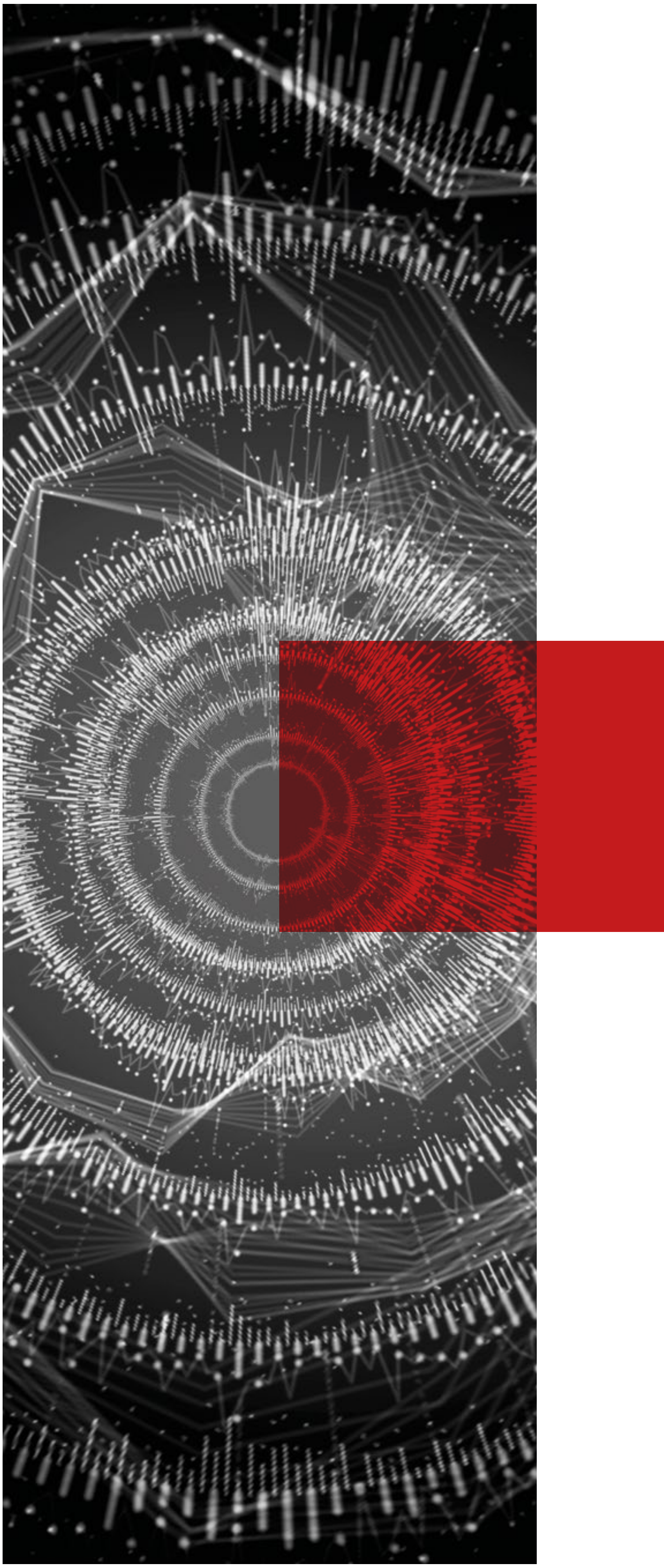
Firstly, Poland has been one of the pace-setters in the cyber defence area, at least in the European part of the Alliance, which was demonstrated e.g. in the course of the

[2] According to the UK Defence Expenditure report from 22 February 2018.

preparations to the 2016 Warsaw NATO Summit during which Poland actively lobbied for recognising cyberspace as an operational domain. Secondly, Poland has been proactive in the cyber defence area over the last decade. Recent decisions made by the Polish government in general and the Ministry of National Defence in particular regarding the consolidation of Polish military cyber capabilities under the auspices of the National Cryptology Centre, the creation of cyber units within the Polish Armed Forces, or the pursuit of development of both defensive and offensive military cyber capabilities confirm Poland's commitment to strengthening cyber resilience and cyber defence. Thirdly, the decision to build the state's cybersecurity system with the Ministry of National Defence in charge, despite being controversial for many reasons, clearly indicates that the Polish government recognises the importance of the military in the overall cybersecurity or cyber defence system.

Also, the goals established by the resolution of the Polish government about 'Detailed directions for rebuilding and modernization of the Armed Forces for years 2017-2026' from June 2018 are in line with the recommendations of the *Strategic Defence Review (Strategiczny Przegląd Obronny)* and are a sign of positive change. They are also a proof of increased awareness in this area. The resolution forms the basis for further work to be done in the defence department, such as the establishment of the Plan of Technical Modernisation for the years 2017-2026. However, even though there is a legal requirement that says the spending on defence should reach 2.5 percent of the GDP until 2030, it still may be insufficient to cover the modernization expenditure required for the Polish army in the coming years.

There are some leading countries in the area of cyber defence, such as the U.S. or Estonia, but none of the Allies is fully ready to face cyberattacks, as none of them is fully resilient. Some of them handle them better than others, but still the challenges are the same for all of them. However, the question is not exactly about the readiness – it is more about the mindset and the situational awareness: there is nothing like being fully ready, there is always a gap that needs to be filled, even in the case of the best performing actors.



NATO's relations with the European Union have been considered as 'Strategic Partnership' since the 2010 Summit in Lisbon. Since the 2016 Summit in Warsaw, the EU has significantly increased its profile and activities in the defence field, predominantly by launching the Permanent Structured Cooperation.

Just before the 2018 Brussels NATO Summit, Secretary General Jens Stoltenberg signed a new Joint Declaration with European Council President Donald Tusk and European Commission President Jean-Claude Juncker, setting out a shared vision of how NATO-EU cooperation can help address most pressing security challenges, including hybrid and cyber threats.

The Summit was an opportunity to enhance further the relationship between NATO and the European Union. The NATO-EU Joint Declaration signed during the 2016 Warsaw NATO Summit highlighted hybrid threats and cyber defence as key areas for cooperation between the two organisations.

The Summit should provide an opportunity to review progress in cooperative projects, as their implementation, not only further declarations, must now be at the heart of the relationship.

There is a Technical Arrangement on cyber defence between NATO Computer Emergency Response Teams and CERT-EU which enables the exchange of information in real time. Both organisations are also members of the Malware Information Sharing Platform that gives them access to each other's databases. Moreover, regular meetings are held during which NATO and the EU representatives share best practices. The results are practical and pragmatic. There is an idea to expand this cooperation within the Technical Agreement.

Both organisations strengthen cooperation in cyber exercises through reciprocal staff participation in respective exercises, including Cyber Coalition and Cyber Europe in particular. Last year, the EU took part in the Cyber Coalition exercises for the first time. Crisis Management Exercises are more of a strategic type of exercises comprising cyber as part of a global defence framework. They are focused on cyber matters in a hybrid environment. In general, this is a good example of strategic and operational cooperation between the two organisations.

NATO Cooperative Cyber Defence Centre of Excellence in Tallinn would probably be the best institution to develop a common NATO-EU framework on how to respond to threats and activities in the cyber sphere.

NATO has reached a turning point when it comes to ensuring its security and the 2018 Brussels NATO Summit was an important opportunity to make the Alliance better equipped to handle emerging new challenges. The Summit lasted two days, but will certainly impact the years ahead. ■

ARTIFICIAL INTELLIGENCE – EMERGING THREATS, CHALLENGES AND OPPORTUNITIES

INTERVIEW WITH MADY DELVAUX-STEHRES

MADY DELVAUX-STEHRES

is a Luxemburgish Socialist MEP. She is Vice-chair of the JURI committee and substitute in the ECON committee. She was rapporteur of the report on Civil Law Rules on Robotics and Chair of the Working Group on Robotics and Artificial Intelligence. Prior to being elected to the European Parliament in 2014, she held various ministerial positions in Luxembourgish Governments over the past 20 years. She was notably Minister for Education and Minister of Social Security, Transport and Communication.

Thank you, Ms Delvaux-Stehres, for finding time for this interview. With the recent advancements in Artificial Intelligence (AI) and machine learning, both new opportunities and threats emerge. AI can empower society, but it in order to do so, it needs smart governance. Given your role as the rapporteur of recommendations to the Commission on Civil Law Rules on Robotics, what is the approach of the European Parliament to this matter? To what extent did the European Commission followed the EP's recommendations in its recently published approach to AI? How to create law flexible enough to embrace the nature of AI and robotics?

Mady Delvaux-Stehres: The plan released a month ago by the European Commission is a step in the right direction, but I think it is not enough. Their communication includes some good points, for instance, the creation of the EU Alliance on AI gathering different stakeholders to monitor the development of these new technologies. I take it as the answer to our call to create a European agency on robotics.

I also very much welcome the decision of the Commission to follow our recommendation to draft a Charter on Ethics, which is expected to happen next year.

But I am disappointed that the Commission does not offer clearer proposals on social aspects such as employment, education, and lifelong learning. Indeed, the proposals underline the importance of these issues, but I'm still missing real action. Expert panels and studies are nice and good tools to better understand the developments in AI, but they are not sufficient to prepare our society for the future.

When it comes to liability, the Commission has only proposed a working document and has not come forward with anything new. This is very disappointing because the time is right for introducing new legislation in order to ensure the EU provides a protecting framework for consumers and legal certainty for companies.

We have been told that a legislative package will be presented next year; however, I believe the EU needs to act now.

Expert panels and studies are nice and good tools to better understand the developments in AI, but they are not sufficient to prepare our society for the future.

AI-based solutions vary across sectors. They may increase productivity, reduce waste and contribute to a higher quality of services. What are the areas of economy where AI-based solutions boost productivity and enhance security the most? How AI could contribute to enhancing the quality of public services? What will, in your opinion, the future job market look like? Will AI create or eliminate more jobs?

The question is: when a company or an institution adopts AI-based tools to increase efficiency, are they confident their employees are skilled enough to use those technologies effectively? Let's take the example of a research project by Assistant-Professor Choudhury at the Harvard Business School involving the United States Patent and Trademark Office. The U.S. patent office has implemented a sophisticated new machine learning program called Sigma-AI. Its aim is to cut the time necessary to review patent applications. Professor Choudhury was interested in finding out whether having a background in computer science and engineering would improve patent workers' ability to use the AI-based tool. He concluded that if someone's past experience had been entirely in the world of older technology, and suddenly a machine learning tool was thrown their way, they would be less productive, even if the tool is great.

This research project shows very clearly the challenges we are facing today. For sure, some jobs will be eliminated, but I think that a vast majority of jobs will remain but their tasks will change in the future. The most crucial part in this process is to ensure extensive training for employees on the one hand and the creation of user-friendly AI-based tools on the other hand.

For sure, some jobs will be eliminated, but I think that a vast majority of jobs will remain but their tasks will change in the future.

Recent disturbing events involving the Cambridge Analytica files showed that we really need to make personal data regulations more stringent to protect our privacy. The adjustment of legislation and technologies is a complicated question. How should AI be regulated in order not to impede innovation and yet guarantee privacy? How to find the right balance between regulation and innovation in order to safeguard privacy?

The General Data Protection Regulation entered into force on 25 May. It will take some time before it is actually possible to draw conclusions on its effect. Some experts already assume that it will not be enough to fully address the problems posed by AI. There is a kind of dilemma in this area. On one hand, the development of AI and robotics requires lot of data; on the other hand, it is essential that we protect our European values, including our right to privacy. As legislators, we sometimes need to resort to artifices to strike a balance, for example, the anonymisation of data which permits companies to develop and secure their products while protecting the privacy of consumers.

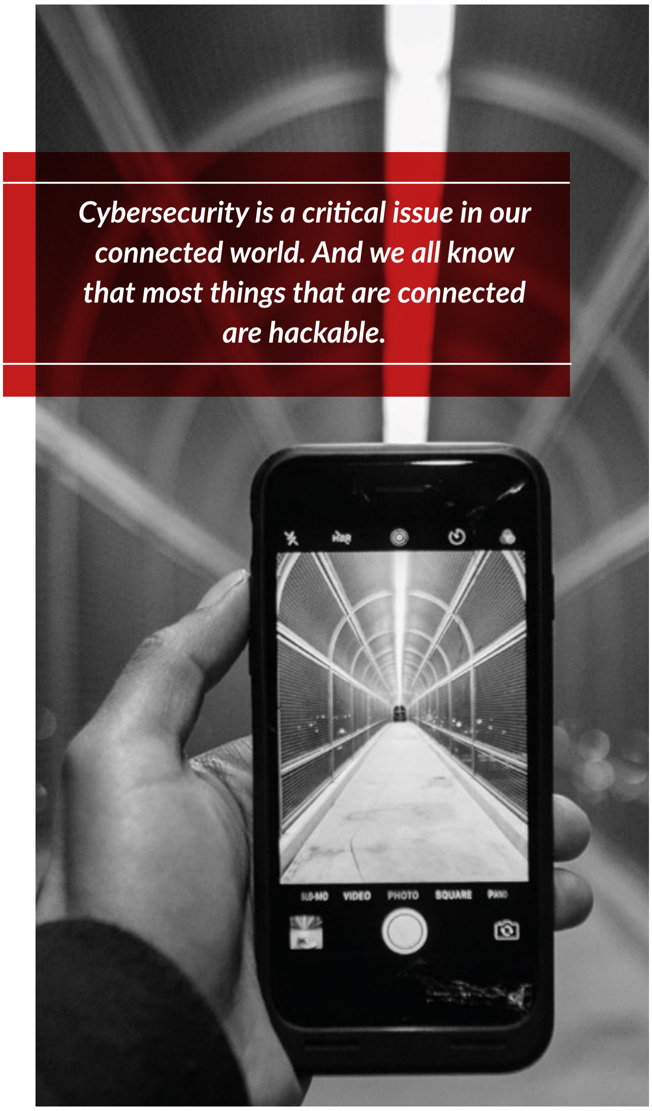
Bearing in mind that both the free flow of non-personal data and a single market for data storage are necessary for the development of AI, what should be done to prevent potential security breaches, cyberattacks and misuse of data? What principles should underline the EU's approach to the cross-border flows of non-personal data?

The Commission has put forward a proposal for a regulation to create a framework for the free flow of non-personal data in the European Union and the foundation for developing the data economy and enhancing the competitiveness of European industry. The challenge is to define clearly what a non-personal data is and to establish the relation between the GDPR and this regulation.

It is a public responsibility to prevent misuse of data and condemn such misuse but it is also the duty of companies to provide the safest possible products and services. It is also in their best interest to do so as the trust of consumers is fundamental in the market.

According to MIT 2018 cybersecurity forecast, this year will see escalation of an AI-driven arms race between hackers and cybersecurity professionals. Security firms and researchers have already been using machine-learning models, neural networks, and other AI technologies for a while to better anticipate attacks, and to detect ones that are already under way. It is highly likely that hackers are adopting the same technology to strike back. How to tip the balance in favour of the 'good guys'? How could the EU contribute to the development of innovative AI-driven cybersecurity solutions?

Cybersecurity is a critical issue in our connected world. And we all know that most things that are connected are hackable. From the political perspective, I think the European Union should boost its investments in Artificial Intelligence and cybersecurity research.



Cybersecurity is a critical issue in our connected world. And we all know that most things that are connected are hackable.

If we want to take part in this new technological race, and be among the best, we have to put a lot of effort into developing security technologies that respect our European values. At the international level, we should work very closely with the International Standard Organisation that is developing standards for the protection of information and ICT.

On 25 April 2018, the European Commission published 'A European Approach on Artificial Intelligence' based on three main pillars: boosting investments, preparing for socio-economic changes, and ensuring an ethical and legal framework. What are, in your opinion, the main challenges for the Commission? What should the process of creating such an approach look like in order to build a safe ecosystem that facilitates the development of AI?

The EU has huge potential in robotics and AI: talented entrepreneurs, motivated research centres, a great consumer market. It is an important opportunity that we have to seize now.

Indeed, we need clear rules to ensure robots serve human interests at all times and the rest of the world is not waiting to be led by Europe on this issue. If we don't decide how we want to shape our future, it is highly likely that China and the USA will decide for us, leaving the EU as simply a follower.

The EU has huge potential in robotics and AI: talented entrepreneurs, motivated research centres, a great consumer market. It is an important opportunity that we have to seize now.

The EU has a duty to stay united and defend our values by taking the lead. By using only soft law and delaying its action, it has incentivised different Member States across Europe to adopt national legislation which endangers our cohesion and risks fracturing the market.

The main challenge for the Commission will be adopting a common EU's approach to create a coherent legal framework providing legal certainty and protecting consumers without stifling innovation.

Many of the world's leading AI researchers and humanitarian organisations are concerned about the potentially catastrophic consequences of developing lethal autonomous weapons. What should be the EU's approach to the so-called 'killer robots'? Is a possible lack of meaningful human control the main concern? On the other hand, how could national defence benefit from AI?

In my opinion, we should ban the use of autonomous weapons altogether. I want to underline that in the report on civil law rules laid down for robotics, we completely excluded 'defence' and 'killer robots'. Given my rather limited background knowledge on these issues, I prefer not to go into further details.

Finally, what are, in your view, the main threats related to AI that are still gaining strength? Are we, as humans, threatened? Or, are you rather optimistic and believe that AI will increase prosperity and the well-being of society?

I believe that technological progress has always contributed to increasing prosperity and the well-being of society. So I am rather an optimist that AI has the potential to do so as well. But since we are talking about the future, and the future is by definition unpredictable, we have to accept that at the end of the day we just don't know what the future will look like.

I believe that technological progress has always contributed to increasing prosperity and the well-being of society. So I am rather an optimist that AI has the potential to do so as well.

As Stephen Hawking said, *"Success in creating effective AI could be the biggest event in the history of our civilisation – or the worst. We just don't know."*

But at least we should be prepared for different scenarios and I'm delighted that the debate is still going on. ■

Questions by Barbara Sztokfisz

ANALYSIS

LIFI – SHINING A LIGHT ON CYBERSECURITY

BY HARALD HAAS, HAMISH STEWART, HARALD BURCHARDT AND NIKOLA SERAFIMOVSKI

PROFESSOR HARALD HAAS

Professor Harald Haas holds the Chair of Mobile Communications in the Institute for Digital Communications (IDCOM) within the School of Engineering at the University of Edinburgh. Professor Haas has published more than 430 peer-reviewed conference and journal papers and his works have been cited more than 22,000 times. He has appeared on the 2018 Thomson Reuters list of highly cited researchers and holds 43 granted patents. He is a Fellow of the Royal Society of Edinburgh, and a Fellow of the IEEE. He holds a Wolfson Research Merit Award. In 2012, Professor Haas received an Established Career Fellowship from the EPSRC, and in 2017 an Established Career Fellowship Extension. Professor Haas is one of the 10 RISE leaders in the UK awarded jointly by the EPSRC and Royal Academy of Engineering in 2014. Professor Haas coined the term 'LiFi' at his first global TED talk in 2011: 'Wireless data from every light bulb'. He is also a co-founder and the chief scientific officer of pureLiFi Ltd, the University of Edinburgh's spin-out company that develops and delivers technology for secure, reliable, high-speed communication networks that seamlessly integrate data and lighting utility infrastructures.

As telecommunications networks evolve and become more complex in order to be able to deal with the requirements of many different users and their required applications, the technologies, processes and controls that are used to build and protect those networks must evolve, too. Here, at the University of Edinburgh and at pureLiFi, we believe that LiFi is one of the technologies that can help do that. LiFi is widely talked about due to its capacity to deliver high-speed data connectivity in densely covered areas, but it should not be forgotten that one of the benefits of LiFi is the ability to constrain the signals within specific areas, thus offering additional security to a wireless network.

Figure 1 shows the spectrum allocation for RF (Radio Frequency) in the UK, but similar allocations can be seen in most countries throughout the world. This RF spectrum is harmonized at the ITU (International Telecommunication Union) for different radio transmission technologies and applications across different countries. Cellular telephone operators use part of this spectrum to provide mobile data services to their users and unlicensed bands are used to provide a variety of services including Wi-Fi. In the last 10 years, the growth in mobile data traffic worldwide has been in excess of 60 percent per year, primarily due to the advent of smartphones. If this trend continues for the next 10 to 15 years, we will need 20 times the entire RF spectrum to satisfy the mobile data demand from users.

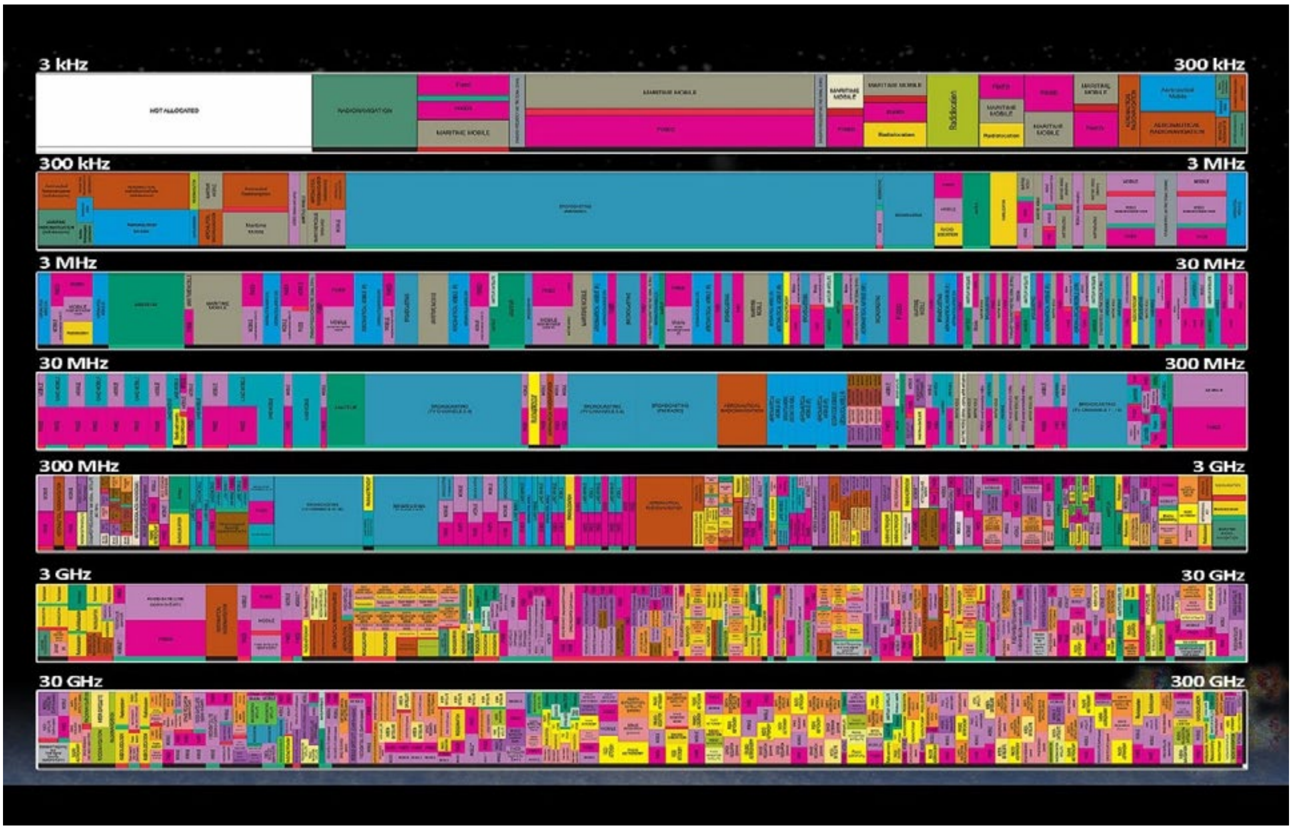


Figure 1. Radio Frequency Spectrum Allocation. Courtesy Ofcom.

There are no reasons to believe that this trend will not continue, or that the demand for wireless spectrum will diminish, indeed the cost of spectrum has increased steadily with each spectrum auction in most countries. We are entering the 4th industrial revolution, and this revolution is driven by data-centric economies and autonomous systems characterised by a fusion of technologies that are blurring the lines between the physical, digital, and biological worlds.

We are moving into the era of 'smart-x', which is based on huge sensor data, signal processing, artificial intelligence, and robotics to create the future autonomous systems that will make our homes, cars, and cities smarter –connectivity is a necessary element in all of these future systems.

We are entering the 4th industrial revolution, and this revolution is driven by data-centric economies and autonomous systems characterised by a fusion of technologies that are blurring the lines between the physical, digital, and biological worlds.

We can compare the fundamental building blocks of these future data-driven systems with real-life intelligent systems where we model the senses (smell, touch, taste, etc.) as sensors (temperature, pressure, vibration, etc.), the brain as a signal processor with memory and the physical interactions as actions or applications. The connectivity between the different parts of these future autonomous systems, largely wireless in nature, will form the 'nervous system', and this nervous system comprising life-saving machines, autonomous cars and mission critical operations has one fundamental challenge to overcome to ensure continued reliable operation – security. How could a human being exist if the information flowing from our senses could not be trusted or could be accessed by others?

Wireless systems built on RF communication present unique challenges when deployed in certain environments, which sometimes lead to vulnerabilities in the system that we believe can be overcome with the use of LiFi.

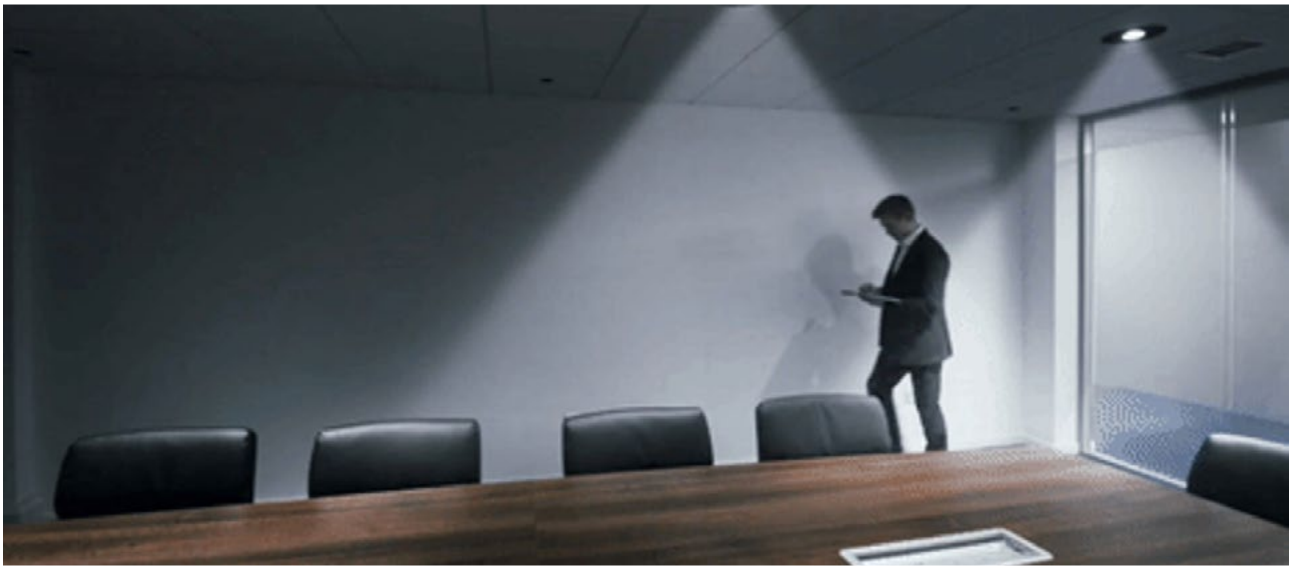


Figure 2. LiFi handover. Courtesy by pureLiFi Ltd.

What is LiFi?

So, what is LiFi and how can it help solve these issues?

The communication industry has witnessed the transition from a communication device, which primarily delivered one service – telephony, to a wireless communication device which delivers hundreds and thousands for services.

The lighting industry is at the dawn of a similar revolution: the incandescent light bulb which provided a single service is being replaced by the LED light bulb. With LiFi, every light bulb becomes a high-speed wireless communication device that uses light to transmit data to a large number of users and sensors in the immediate environment.

LiFi, shown in Figure 2, is a new wireless communications technology that fuses together these two industries to provide a high-speed, bi-directional and networked delivery of data through light. LiFi uses light to send data to end-user devices (typically using the visible light spectrum), and back from the end-users devices to the luminaires (typically using the invisible infrared spectrum). When a device moves out of the light cone of one light, the services can be handed over to the next light, a principle called 'handover' in modern cellular systems providing seamless connectivity to the end-user device. This is what we invented and called 'LiFi'.

LiFi is a new wireless communications technology that fuses together these two industries to provide a high-speed, bi-directional and networked delivery of data through light.

Advantages of LiFi

LiFi has a number of unique advantages when compared to traditional RF-based communication systems, some of which lend themselves well to improving cybersecurity in a wireless network.

Physical layer security

LiFi enhances physical layer security by at least an order of magnitude when compared to RF. Moreover, it allows entirely new cybersecurity enhancing techniques to be applied in networks. This is due to the fact that light can be relatively easily contained in a physical location, which is not the case in radio-based systems. This feature is also instrumental in providing very precise localisation information, thus further enhancing wireless cybersecurity.

Figure 3 shows an example of how LiFi increases physical layer security. The building on the left is fitted with four Wi-Fi access points, one in each room, to provide wireless connectivity, whereas the building on the right is fitted with four LiFi access points, also one in each room, to provide wireless connectivity.

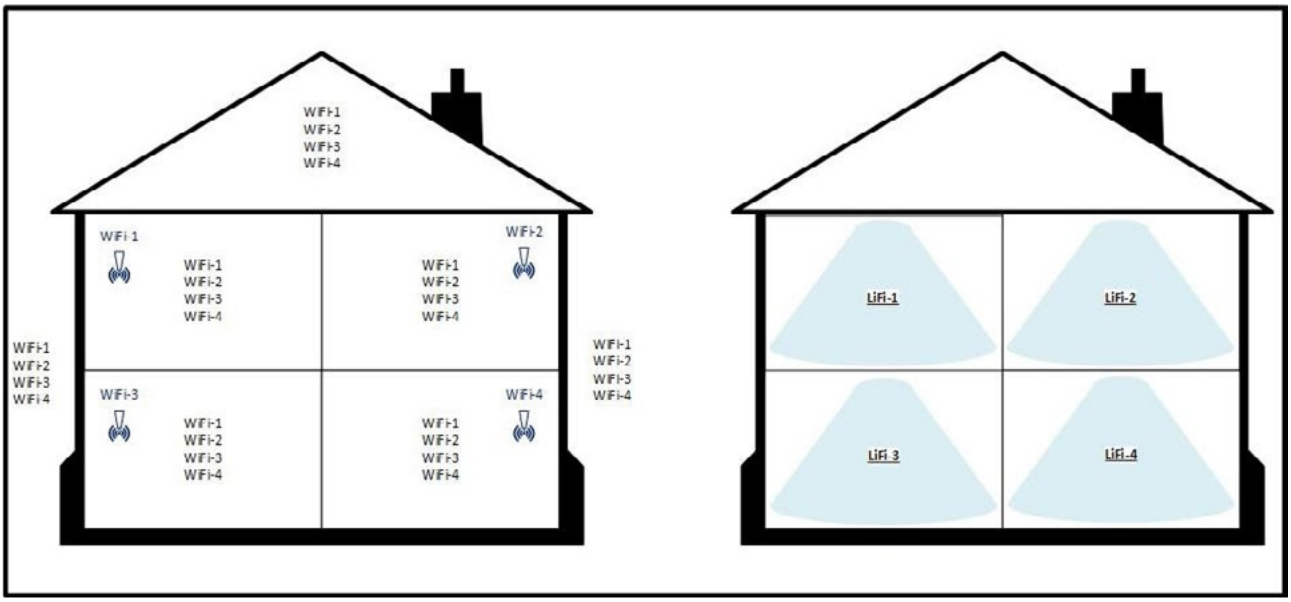


Figure 3. LiFi physical layer security. Own Graphic.

In the building with Wi-Fi connectivity, signals from all four access points can be seen in all rooms; in fact, they can even be seen in the roof space and outside of the building. By contrast, in the building with LiFi connectivity, the signal from each LiFi access point is contained entirely within the room in which it is installed because light does not travel through walls. This means that all LiFi signals from the neighbouring rooms cannot be seen by each other, adding a layer of security to the light-based wireless system that offers better protection than radio-based wireless system where all the Wi-Fi signals from the surrounding environments can be received. This is a phenomenon that can be seen today in homes, offices, shopping malls and high streets where a long list of available Wi-Fi networks often appears on your smartphone when you attempt to connect to a specific network. This will not be observed in LiFi-based wireless networks as the signals are contained to the location where the light can be seen.

In the building with LiFi connectivity, the signal from each LiFi access point is contained entirely within the room in which it is installed because light does not travel through walls.

Network data density and Geo-fencing

LiFi allows orders of magnitude improvements in data density when compared to radio-based systems like Wi-Fi; this is important when many devices need to be connected securely to a network in very close proximity to each other and at very high speeds.

Figure 4 shows a typical floor plan of a security conscious office environment where the rooms are used for different functions by different people – all of whom may require different levels of security access. For example, a General Operations space may need more 'lenient' access rights to the network than the Commanders Office, while a Secure Files location may require the highest level of security to be provided to a restricted pool of employees. If wireless connectivity was provided to the network using Wi-Fi, then the signals would permeate the entire floor space, which would make it very difficult to secure individual locations and user access. However, as shown in the diagram, the circles represent how LiFi could be deployed across the floor with each circle representing a LiFi access point/luminaire that provides wireless connectivity to a specific desk or user.

The partitioning of access rights can easily be accomplished with LiFi since the lights in the Commander's Office do not spread over into the General Operations Space, assuming that walls or even opaque barriers typically separate these areas. This limited physical access allow simple implementation of geofencing concepts.

In addition, since light is spatially contained, dual-gate locking can be used where the location of the user and

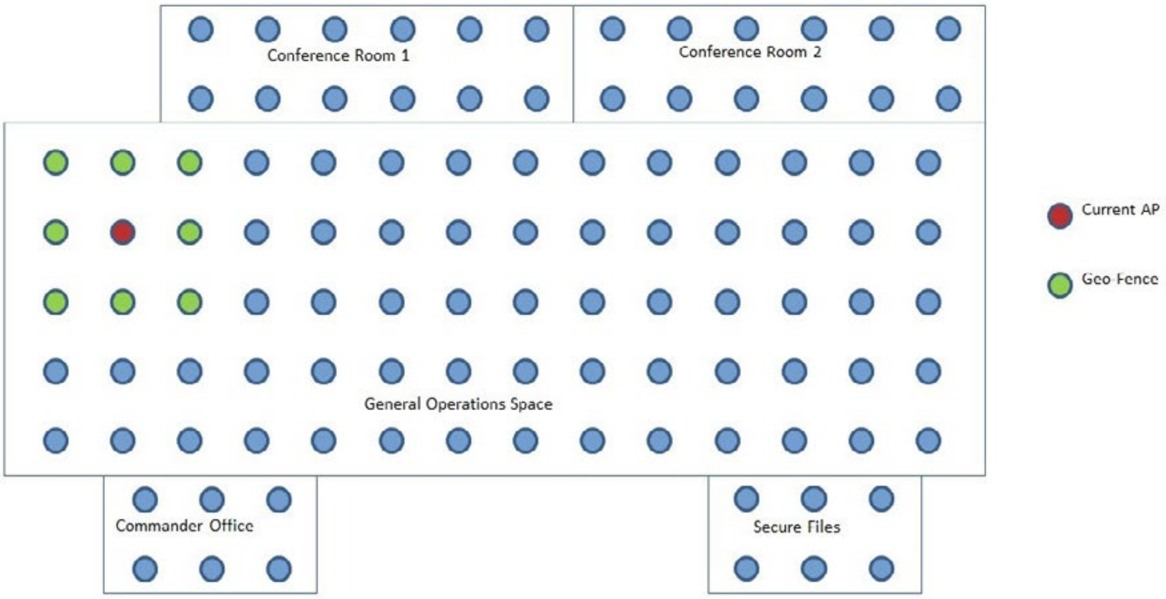


Figure 4. Network density and Geo-location. Courtesy by pureLiFi Ltd.

the location of the light in the physical world are used to determine the access privileges of a user. The result of implementing such a feature in the LiFi network is that someone sitting outside the 'fence' would physically be restricted from accessing the devices connected within the fence if they did not have the correct level of security. This means that security threats, such as 'man-in-the-middle' attacks, would be significantly reduced – if not eliminated altogether.

The network can also be adaptive, making the geo-fenced location actually move around the office in real time as users are moving from one location to another. Unlike traditional wired access, where the access of a data port is fixed regardless of the physical location of the user, a LiFi system can chose to provide access to a user only if they are proven to be in the given area and only if their device is "legitimately" moved within the system. In Figure 4, this would mean that for the user to gain access to files available in the Commander's office, they would need to move from the red AP to the green AP. As the user moves from the red AP to the green AP, the LiFi system would adjust their new neighbourhood and the user would be allowed to move to another location. In this manner, when a user leaves the immediate neighbourhood of their connected light, then their access credentials are no-longer valid and therefore a motivated attacker could not access their files.

> ***LiFi system can chose to provide access to a user only if they are proven to be in the given area and only if their device is "legitimately" moved within the system***

Operation in RF hostile environments

LiFi works in intrinsically safe environments such as petro-chemical plants, nuclear power plants and gas pipework installations – in other words, conditions where a spark from or to the radio antenna of a user device can cause an explosion or interrupt processes that could lead to significant economic or even life-threatening consequences. In addition, unlike RF, LiFi can work effectively under water.

In Atlanta, at a first responders training facility, LiFi was presented as a life-saving technology for first responders, helping to maintain communications in a subway attack. At an event named Operation Convergent Response (OCR), held at the Guardian Centers training facility in the United States, pureLiFi demonstrated their wireless LiFi technology in a subway disaster scenario. The Guardian Center is a world class U.S. training facility where disaster response units can gain experience under real emergency conditions.

The LiFi technology was used to maintain real-time and bi-directional communications with a command centre, allowing the emergency services to maintain safe and reliable connectivity during a response.

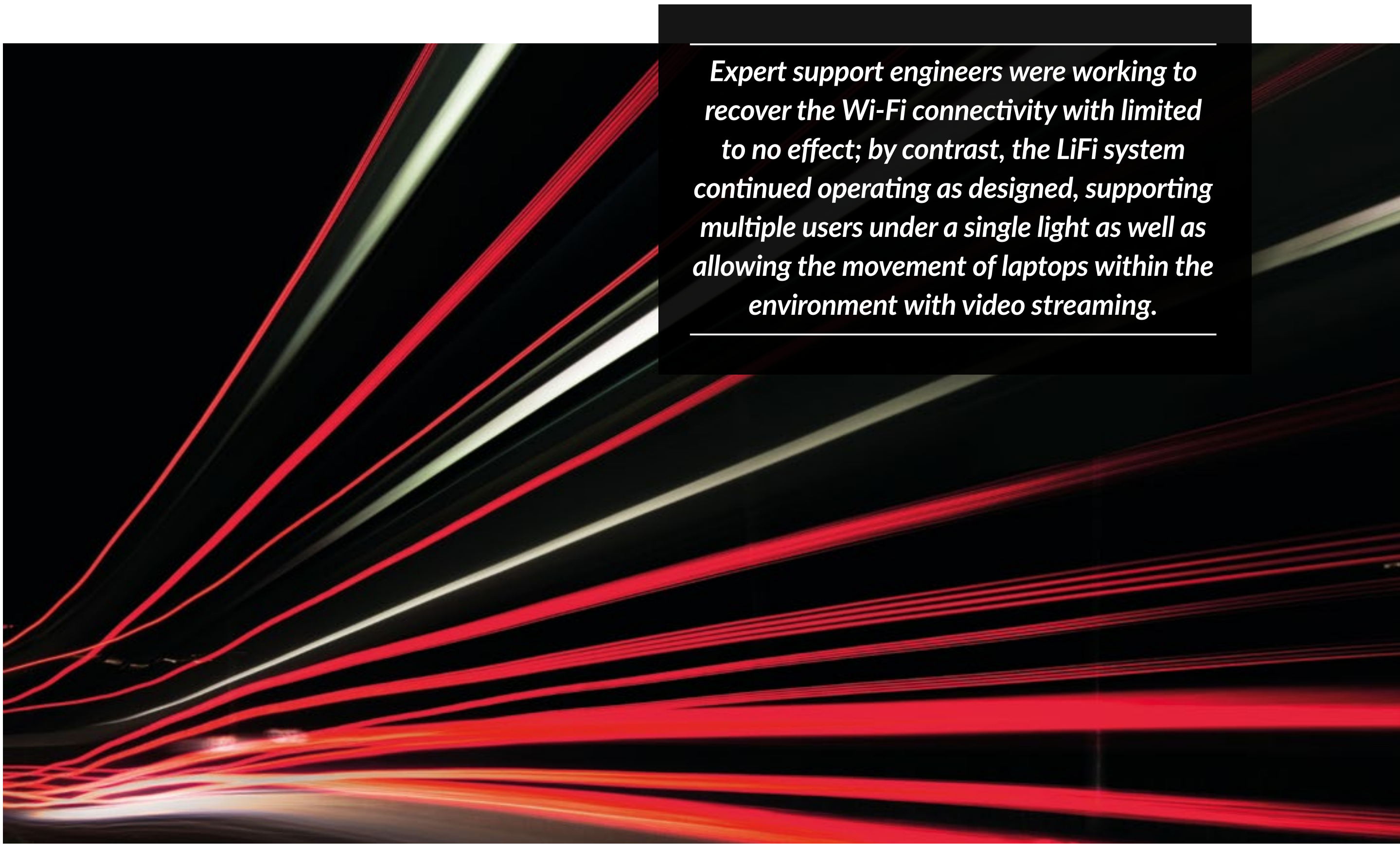
pureLiFi have also deployed the LiFi-X system during a live exercise with the UK Joint Forces Command at Joint Venture 2016 alongside BT, Cisco, Antillion and others to demonstrate the Secure Wireless Headquarters of the Future. The aim was to show a wirelessly connected environment that could be rapidly deployed in the field while ensuring the appropriate level of security and data restriction. A local server and a switch infrastructure were used with a secure Wi-Fi system deployed alongside the LiFi-X system to cover a single tent. A total of 20 laptops were used in the exercise, with 10 connected to the Wi-Fi network and 10 connected to the LiFi network. Each laptop required network connection to remain logged in and provide access to the collaborative working environment.

The demonstration involved active MoD staff who were asked to complete the day's exercise in the wireless environment. In addition, an EMI monitoring unit was deployed to assess the RF signature and system vulnerability. All systems were operational before the start of the exercise, but the Wi-Fi connectivity was lost and all systems operating on Wi-Fi were down at an early stage of the event. Expert support engineers were working to recover the Wi-Fi connectivity with limited to no effect; by contrast, the LiFi system continued operating as designed, supporting multiple users under a single light as well as allowing the movement of laptops within the environment with video streaming.

The LiFi system enabled a complete redesign of the operational environment with no impact on the network design and architecture and the exercise was completed successfully with work entirely reliant on the LiFi system for connectivity.

At the debriefing session following the exercise, the reason for the Wi-Fi failure was identified as a single £100 home-made dual-band (2.4 GHz and 5 GHz) jamming device that was hidden near the tent. A special unit tasked with disrupting the exercise had successfully triangulated the tent from at remote position and was able to capture and block the encrypted Wi-Fi signal without the use of UAVs.

Expert support engineers were working to recover the Wi-Fi connectivity with limited to no effect; by contrast, the LiFi system continued operating as designed, supporting multiple users under a single light as well as allowing the movement of laptops within the environment with video streaming.



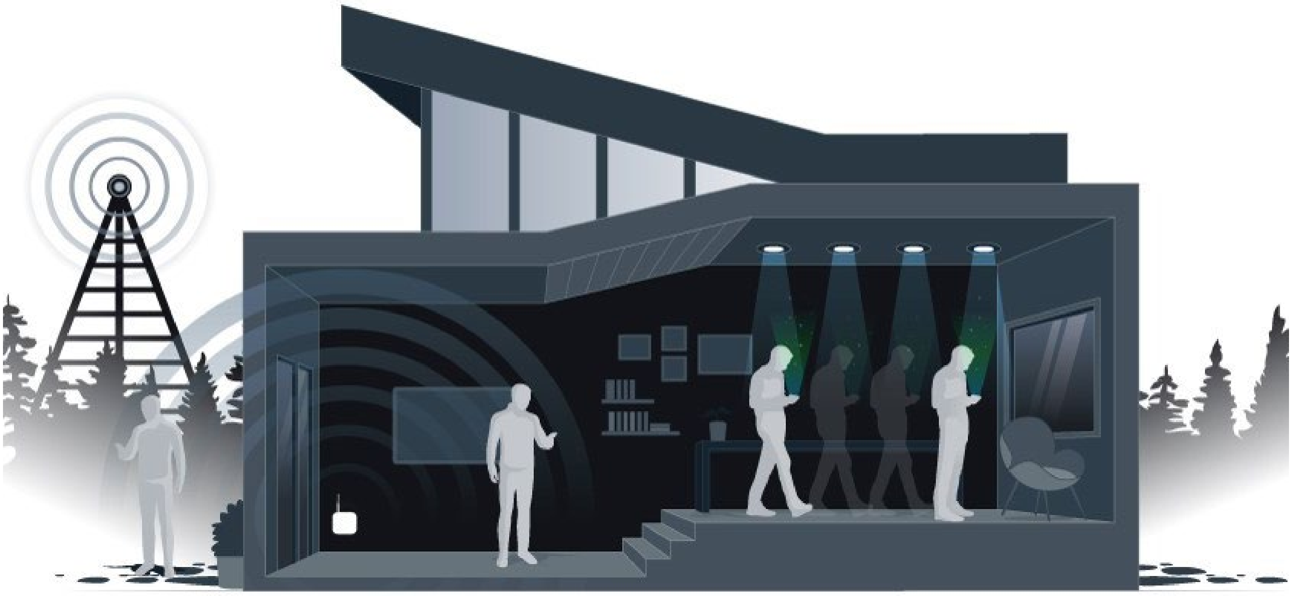


Figure 5. LiFi in the real world. Courtesy of pureLiFi

The EMI monitoring unit was unable to detect the radiation from the LiFi system and a LiFi signal was inaccessible and invisible outside of the operating environment, even within the same tent.

The exercise showed that LiFi was immune to traditional RF jamming and RF monitoring while offering an unprecedented level of information confinement and rapid deployment. The LiFi system was able to deliver a user experience similar to traditional Wi-Fi within a strictly defined environment offering all the benefits of a cabled connection with the flexibility of a wireless network.

LiFi in the real world

LiFi is not just a concept; it is a revolutionary wireless communications technology being deployed today and used all over the world. Figure 5 shows how LiFi seamlessly integrates into existing wireless networks, enabling fast handover from cellular networks to Wi-Fi networks and to LiFi networks. LiFi is not a technology of the future, it is a technology component helping to future-proof wireless connectivity which offers additional layers of security. ■

ANALYSIS

SECURING IOT – ENABLED SMART CITY SERVICES – THE MILITARY PERSPECTIVE

MAURO TORTONESI

Mauro Tortonesi is an Assistant Professor at the Department of Engineering of the University of Ferrara in Ferrara, Italy. His main research activities focus on communications and management solutions for Internet of Things (IoT) applications in military and industrial environments, collaboratiion with the United States Army Research Lab, the Florida Institute for Human & Machine Cognition, and the R&D divisions of many world leading manufacturers, such as Carpigiani Group, FIAT Chrysler Automobiles, etc. Dr Tortonesi's research interests also include cloud computing, opportunistic networking, IT service management, and business-driven IT management. He has authored or co-authored more than 60 scientific papers and served in technical program committees of dozens of international conferences and workshops. He co-chaired several international conferences and workshops in the IT management research area. Dr Tortonesi acted as a reviewer for 14 international research journals and sat on the editorial board of 2 international research journals. He is also a member of IEEE and ACM.

Introduction

In the near future, Smart Cities are expected to provide their digital citizens with intelligent resource utilisation solutions for energy, water, mobility, parking spaces, as well as a new generation of real-time and time-critical, location-, social-, and context-aware services for healthcare, entertainment, and social good (Khatoun and Zeadally, 2016).

Most (if not all) of these applications leverage the functions of Internet of Things (IoT) devices operating as a capillary network of sensors providing a constant stream of information (Al-Fuqaha et al., 2015). The deluge of data generated by IoT applications and devices is estimated by Cisco to reach 850 ZB by 2021 (Cisco, 2018).

Traditional analytic solutions based on transferring all the data to the cloud, processing them using big data methodologies and tools, and returning the results to interested users are too slow for applications with strict latency constraints, and too burdensome for the network infrastructure. Instead, the Smart City scenario is particularly well suited for the adoption of distributed processing approaches, such as fog computing, in which information processing services are executed on edge devices in proximity of either raw data sources, information consumers, or both (Mukherjee, Shu, and Wang, 2018).

In the near future, the widespread adoption of IoT technologies in Smart City scenarios will raise significant security issues. In fact, the multitude and pervasiveness of IT services provided by Smart Cities will present a massive attack surface whose protection will require the development of cybersecurity solutions not only in the IT domain, but also in Operational Technology (OT).

In the near future, the widespread adoption of IoT technologies in Smart City scenarios will raise significant security issues.

Industry and academia have long recognised security as a fundamental pillar for the realisation of Smart City platforms and have been very active in designing cybersecurity solutions for Smart City scenarios that leverage their extensive experience in corporate IT and in IoT applications and networks. Recently, the military have also started paying special attention to the opportunities and challenges brought by the IoT (Suri et al., 2016).

In fact, the military are currently investigating an interesting role that the IoT can play as a foundation for building new capabilities in battlefield scenarios (Kott, Swami, and West, 2016). More importantly, the military also expect the IoT to become a significant source of information for military operations in urban environments (Tortonesi et al., 2016). Smart City infrastructure systems, such as traffic monitoring systems, smart utility networks, public transportation systems, video surveillance networks, and other services originally designed to improve the quality of life of citizens might become, from the situational awareness perspective, very valuable in military operations, possibly making purposely built and deployed sensors unnecessary, or even obsolete.

These assets would especially help Humanitarian Assistance and Disaster Recovery (HADR), counter-terrorism, and mass protection scenarios. In fact, so far most HADR operations had to leverage on purposely deployed ad hoc communication systems with limited or no connection to IT infrastructures in the affected cites, with less than ideal results in terms of operational effectiveness, response times, and costs. At the same time, counter-terrorism operations would benefit immensely from the access to the monitoring assets of Smart Cities, such as traffic cameras.

Securing Smart Cities: A Holiday Celebration Example

To illustrate how Smart Cities could contribute to more comprehensive intelligent solutions to support the security of their citizens, let us consider how IoT-based services could ensure the citizens' security during a holiday celebration in a Smart City environment.

In preparation for the usual gathering of a large crowd, a section of the city centre will be closed to automobile traffic and will be accessible only to pedestrians. To support the Emergency Medical Services (EMS) personnel and police forces deployed to guarantee the safety of the citizens, a smart security IT infrastructure will be activated. A pool of security focused applications will continuously analyse the data collected from a wide range of IoT information sources, such as traffic cameras, usually dedicated to day-to-day monitoring of the city, to maintain an accurate and always up-to-date situational awareness and to produce actionable knowledge. Those applications will run on a dedicated fog computing platform that allows the instantiation of software components on either a suitable edge device or in the cloud, according to the application requirements and the current network conditions.

More specifically, we can envision several applications concurrently running in the Smart City fog computing platform, each one leveraging a specific set of IoT generated data and of IT services and competing for the available computational and bandwidth resources. First, a logistics support application will provide an accurate and up-to-date estimate of the number of people present in the city centre, by cross correlating information such as the number of personal devices (smartphone, wearables, etc.) currently connected to the network and the count of persons appearing on image and video camera feeds collected from IoT devices. This information will help to plan the allocation of EMS personnel and resources (public water services, hygiene spots, ambulances, etc.).

In addition, a security check application will help police forces to quickly identify obvious and/or evident security threats, such as a person wielding a weapon or a group of people starting a brawl, by continuously analysing image and video feeds collected from, e.g., traffic cameras. To automatically identify anomalies in the shortest possible amount of time, the application will take advantage of both the low-latency processing allowed by the fog and the computational capabilities of the cloud and run with the highest possible priority and possibly no associated resource consumption constraints. More specifically, the application will implement a first-order security control service in the fog that runs coarse-grained anomaly detection algorithms with relatively light computational requirements on the data collected by IoT devices. At the same time, the application will implement a second-order security control service in the cloud, running more fine-grained face recognition algorithms against a database of known people, in order to help the police to identify less evident and potentially more dangerous security risks, e.g., for counter-terrorism purposes.

Other e-health applications will leverage the Smart City fog computing platform to support EMS personnel in delivering medical services. For instance, an application might try to early identify possible health emergencies, such as heat strokes and dehydration, by cross-correlating data collected from IoT devices (traffic cameras, temperature sensors, etc.), wearable devices (smart bracelets monitoring heartbeat rate, sweat presence, and other physiological activities, etc.), a mobile devices (running apps such as pace monitors, fall detectors, and so forth).

Finally, public service applications and commercial applications can also be run on the fog computing platform. For instance, a smart mobility application could provide useful information to citizens by disseminating traffic information or suggesting which underground train to take in order to get quickly outside of the city centre. Other applications could provide services that integrate with IoT sensors, identifying impromptu performances from street artists or particularly interesting shopping sales, and directing users to their locations.

These applications operate on a wide range of data types and present different requirements for the information processing tasks. Facilitating their development requires an innovative information model and a corresponding information-centric and value-based service framework to deal with the main challenge of Smart City environments, i.e., the capability to process the deluge of continuously generated raw data. At the same time, there is a need for comprehensive fog computing solutions capable of implementing coherent and homogeneous management functions for a plethora of different services running on diverse but federated cloud and fog environments.

These applications operate on a wide range of data types and present different requirements for the information processing tasks. Facilitating their development requires an innovative information model and a corresponding information-centric and value-based service framework to deal with the main challenge of Smart City environments.

Challenges

Realising smart security applications, such as the one described in the previous section, presents many specific challenges.

First, there is the issue of federating Smart City platforms with police, civil protection, and military force systems. A carefully planned coordination between military and civilian organisations might allow for the implementation of *a priori federation* of identity and access management in Smart City services and assets, enabling emergency response teams to leverage them when needed, according to a predefined security policy, and possibly also implementing partial data anonymization and/or purging to preserve the citizens' privacy. Alternatively (or complementarily), Smart City platforms might be designed to enter in a 'break glass' emergency mode when needed. 'Break glass' security policies, conceived to handle severe emergency situations, implement a complete override of standard security policies. When operating in a 'break glass' mode, Smart City platforms should execute strict auditing and logging measures, enabling the *a posteriori* analysis of operations performed during emergencies, and consequently facilitating their recovery to regular operations.

In addition, there is the issue of interoperability, not only in terms of data representation formats and communication protocols, but also (and perhaps more importantly) of asset discovery and Application Programming Interfaces (APIs) to access open data sources. Despite the impressive results achieved by a few outstanding initiatives, such as the Forum Virium in Helsinki, the lack of standardisation in this area is widely recognised as a major obstacle to the realisation of IoT-based Smart City applications. To address this issue, at the recent 2018 World Forum on the IoT in Singapore, the IEEE has launched a standardisation effort for Smart City protocols.

Information assurance represents another important issue. In fact, leveraging information from commercially deployed IoT systems in Smart Cities and other unknown and/or uncontrolled IT infrastructures raises possible issues of information distortion in the gathered data. While that information might be very valuable from a situation awareness perspective, it should not be treated as entirely reliable and decision-makers should be clearly informed about its possibly untrustworthy nature.

Last but not least, there is the problem of taming the formidable deluge of data generated by Smart City services and IoT assets to provide actionable knowledge through accurate and low-latency analytics. Traditional centralised solutions, based on big data analytics running in cloud computing platforms, fall well short of accomplishing this ambitious goal. There is a need, instead, to consider new solutions at the information and service model level that explore several trade-offs between processing speed and accuracy.

Federation, interoperability, and trustworthiness issues are further exacerbated by the coexistence and co-deployment of a military system and commercial IoT solutions (Tortonesi et al., 2016). This integration, which might be unavoidable in HADR scenarios, raises serious cybersecurity and compatibility concerns.

Solutions

Military research has offered many interesting solutions. First of all, the researchers at the United States Army Research Lab (ARL) are arguably leading the investigation of Value of Information (VoI) based methodologies and tools within the computer network research community.

The birth of the VoI concept, which measures the utility of information according to a subjective and consumer-centric perspective, can ultimately be traced back to the seminal work by Howard that attempted to extend Shannon's information theory to consider both "the probabilistic nature of the uncertainties that surround us, but also with the economic impact that these uncertainties will have on us" (Howard, 1966). Having been an active research topic in economic and decision-making theories for the last 50 years and still receiving a considerable amount of attention, the investigation of utility that each discrete element of information provides to its consumer(s) holds interesting promises for several application scenarios, including the IoT and Smart City (Suri et al., 2015).

In fact, classifying information according to the value it provides to its recipients represents a natural and very effective criterion to discard data whose processing or dissemination is not allowed due to a limited amount of resources available as well as to prioritise the utilization of data collected from more reliable sources.

Building upon the VoI concept, military research has fostered the development of innovative platforms, such as SPF (as in 'Sieve, Process, and Forward'), to address the issues of IoT applications in Smart City environments (Tortonesi et al., 2018). The SPF advocates the adoption of an 'acceptable lossyness' perspective for the realisation of IoT-based services, leveraging VoI-based prioritisation to deliver high levels of Quality of Experience (QoE), even in resource scarce environments. To this end, the SPF proposes an innovative information model and a corresponding information-centric and value-based service framework to deal with the main challenge of Smart City environments, i.e., the capability to process the deluge of continuously generated raw data.

> ***Classifying information according to the value it provides to its recipients represents a natural and very effective criterion to discard data whose processing or dissemination is not allowed due to a limited amount of resources available as well as to prioritise the utilization of data collected from more reliable sources.***

Finally, other methodologies and tools that were proposed within the NATO IST-147 Research Task Group on Military Applications of the IoT include solutions for the 'pedigree' tracking of sensing information and related visualisation techniques, the involvement of civilians in rescue operations, security solutions for information coding (Wrona, De Castro, and Vasilache, 2016) and communication link (Furtak, Zielinski, and Chudzikiewicz, 2016) layers, etc. (Johnsen et al., 2018).

However, these solutions often leverage models that represent a significant paradigm shift with respect to the currently proposed approaches. As a result, there is still much work to be done to validate them as building blocks of the next generation smart security applications.

Conclusions

The widespread adoption of the IoT in Smart City applications presents compelling opportunities to increase the security of citizens, but their realisation poses several challenges at various levels: IT service design, architecture, and integration. Like industry and academia, the military are well aware of the opportunities and challenges brought by the IoT and currently investigating these problems through innovative methodologies and tools (Suri et al., 2018).

It is perhaps too early to say if the increasing interest in the adoption of the IoT in the military will lead to a new era of IoT-enabled operations and the emergence of innovative and sophisticated cyber-physical applications, just as the advent of communications networks ushered in the era of network-centric warfare. However, the military are hard at work to prepare for possible Humanitarian Assistance and Disaster Recovery (HADR), counter-terrorism, and mass protection scenarios, and are increasingly looking towards the IoT as an extremely valuable, although not entirely reliable, information source for situational awareness purposes. ■

REFERENCES

Al-Fuqaha, A. et al. (2015). Internet of Things: A Survey on Enabling Technologies, Protocols, and Applications. *IEEE Communications Surveys & Tutorials.* 17(4). 2347-2376.

Cisco global cloud index: Forecast and methodology, 2016-2021. (2018). Cisco.

Furtak, J. Zielinski, Z., and Chudzikiewicz, J. (2016, December 12-14). Security techniques for the WSN link layer within military IoT. IEEE 3rd World Forum on Internet of Things (WF-IoT 2016). Reston, VA, USA.

Howard, R. (1966). Information value theory. *IEEE Transactions on Systems Science and Cybernetics.* 2(1). 22-26.

Johnsen, F. et al. (2018, May 22-23). Application of IoT in Military Operations in a Smart City. Proceedings of the 2018 International Conference on Military Communications and Information Systems (ICMCIS 2018). Warsaw, Poland.

Khatoun, R. Zeadally, S. (2016, July). Smart cities: concepts, architectures, research opportunities. *Communications of the ACM.* 59(80). 46-57.

Kott, A. Swami, A. and West, B. J. (2016). The Internet of Battle Things. *Computer.* 49(12). 70-75.

Mukherjee, M. Shu, L., and Wang, D. (2018, in press.). Survey of Fog Computing: Fundamental, Network Applications, and Research Challenges. *IEEE Communications Surveys & Tutorials.*

Suri, N. et al. (2015, October). Exploring Value of Information-based Approaches to Support Effective Communications in Tactical Networks. *IEEE Communications Magazine.* 53(10). 39-45.

Suri, N. et al. (2016, May 23-24). Analyzing the Applicability of Internet of Things to the Battlefield Environment. Proceedings of the 2016 International Conference on Military Communications and Information Systems (ICMCIS 2016). Brussels, Belgium.

Suri, N. et al. (2018, February 5-8). Exploring Smart City IoT for Disaster Recovery Operations. Proceedings of 2018 IEEE 4th World Forum on Internet of Things (WF-IoT 2018). Singapore.

Tortonesi, M. et al. (2016, December 12-14). Leveraging Internet of Things within the military network environment – Challenges and solutions. Proceedings of 2016 IEEE 3rd World Forum on Internet of Things (WF-IoT 2016). Reston, VA, USA.

Tortonesi, M. et al. (2018, in press.). Taming the IoT Data Deluge: An Innovative Information-Centric Service Model for Fog Computing Applications. *Future Generation Computer System.*

Wrona, K. De Castro, A., and Vasilache, B. (2016, December 12-14). Data-centric security in military applications of commercial IoT technology. Proceedings of 2016 IEEE 3rd World Forum on Internet of Things (WF-IoT 2016). Reston, VA, USA.

CYBERSEC

EUROPEAN
CYBERSECURITY FORUM

DON'T MISS THE 4TH EDITION

SAVE THE DATE 8–9 OCTOBER 2018

FOLLOW US ON:

#CSEU18

WWW.CYBERSECFORUM.EU

ANALYSIS

BLOCKCHAIN SECURE CLOUD: A NEW GENERATION INTEGRATED CLOUD AND BLOCKCHAIN PLATFORMS – GENERAL CONCEPTS AND CHALLENGES

JOANNA KOŁODZIEJ

is the Professor of computer science and Head of the Computer Science Department at Cracow University of Technology. She works also in Research and Academic Computer Network (NASK) Institute. Prof. Kołodziej serves as the President of the Polish Chapter of IEEE Computational Intelligence Society. She participated in several international and national projects including ECONET, 7FP and PARAPHRASE 7FP Grants. Currently, she is the Principal Investigator of Horizon 2020 cHiPSet Cost project IC1406 (chipset-cost.eu). She is the leader of the Polish consortium of BalticSatApps EU InterReg project (http://balticsatapps.eu/). Prof. Kołodziej is the author and editor of 20+ books and the author of 170+scientific publications in top world international journals in the area of computer science and applied mathematics.

ANDRZEJ WILCZYŃSKI

is an Assistant Professor at Cracow University of Technology and Ph.D. student at AGH University of Science and Technology. The topics of his research include blockchain-based modelling in distributed computing, cloud computing, in particular data and resource virtualization, tasks scheduling in cloud computing and broadly defined security in these areas.

DAMIÁN FERNÁNDEZ-CERERO

received the B.E. degree and the M.Tech. degrees in Software Engineering from the University of Sevilla. In 2014, he joined the Department of Computer Languages and Systems, University of Seville, as a Ph.D. student. In 2016 he was invited by at ENS-Lyon and in 2017 at Cracow University of Technology to work in saving energy solutions for cloud infrastructures. Currently he both teaches and conducts research at University of Sevilla. He has worked on several research projects supported by the Spanish government and the European Union. His research interests include energy efficiency and resource scheduling.

ALEJANDRO FERNÁNDEZ-MONTES

received the B.E. degree, M. Tech. and International Ph.D. degrees in Software Engineering from the University of Sevilla, Spain. In 2006, he joined the Department of Computer Languages and Systems, University of Sevilla, and in 2013 became Assistant Professor. In 2008 and 2009 he was invited to the ENS-Lyon, in 2012 to the Universitat Politecnica de Barcelona and in 2016 to Shanghai Jiao Tong University for share experiences and knowledge in saving energy solutions for Data Centers. His research interests include energy efficiency in distributed computing, applying prediction models to balance load and applying on-off policies to Data Centers.

Introduction

As we delve deeper into the 'Digital Age', we witness an explosive growth in the volume, velocity, and variety of data available on the Internet. For example, in 2012, about 2.5 quintillion bytes of data were created each day. The data originated from multiple types of sources, including mobile devices, sensors, individual archives, social networks, the Internet of Things, enterprises, cameras, software logs, etc. Such 'data explosions' have raised one of the most challenging research questions of the current Information and Communication Technology (ICT) era: how to effectively and optimally manage such large amounts of data and identify new ways to analyse them in order to unlock information.

Millions of financial transactions realised each day in today's global market generate hundreds of petabytes of sensitive heterogeneous data, which requires it to be processed efficiently (stored, distributed, and indexed) in a way that does not compromise end-users' Quality of Service (QoS) in terms of data availability, data privacy, data search delay, data analysis delay, and the like. Many of the existing ICT systems that store, process, distribute, and index hundreds of petabytes of heterogeneous data fall short of this challenge or simply do not exist yet. There has been a paradigm shift in executing high-performance large data applications from physical hardware- and software-enabled platforms managed locally, which should be processed, analysed and stored in safe ICT environments.

The main research challenge in the ICT support of the financial markets is the development of a next generation financial technology for a secure use of electronic currencies and a secure network technology for system user communication, as well as data processing and storage without the involvement of third parties. To deal with the security aspects of financial virtual transactions, *blockchain* technology has been proposed. Blockchain can be defined as a public ledger network for secure online transactions with virtual currencies. Transaction records are encrypted by using cryptographic methods and executed in a distributed computer network as blockchain software.

The blockchain model has been gaining popularity since 2008, when the first electronic money protected through the cryptographic mechanisms (cryptocurrencies) was introduced. The first cryptocurrency to use a blockchain-based approach was Bitcoin (Il-Kwon et al., 2014). These currency blockchain systems store the value attached to a digital wallet—an electronic device (or software) that allows realising electronic transactions.

Blockchain transactions are finalized through an authentication process, where the customer who borrows virtual money creates a block of transactions. This block is periodically updated and reflected in the electronic money transaction details to share the latest transaction detail block (Armknecht et al., 2015).

Blockchain can be successfully utilised in diverse areas, including the financial sector and the ICT computational environment, such as computational clouds (Christidis and Michael, 2016), (Huh et al., 2017). Cloud computing gives application developers the ability to marshal virtually infinite resources with an option to pay-per-use and as needed and does not require upfront investments in resources that may never be optimally used. Once applications are hosted on cloud resources, users are able to access them from anywhere, at any time, using devices ranging from mobile devices (smartphones, tablets) to desktop computers. The data centre cloud provides virtual centralisation of applications, computing, and data. While cloud computing optimises the use of resources, it does not (yet) provide an effective solution for the secure hosting of large data applications (Singh et al., 2016).

In this paper, we define the generic model and the main characteristics of the blockchain network. We present it as a reference infrastructure, which can be easily combined with other large-scale distributed computational environments. We briefly discuss the concept of integration of blockchain with cloud platforms in order to improve the security of data storage as well as resource, data and user management in both environments.

Blockchain origins

Blockchains can be defined as distributed digital ledgers of cryptographically signed transactions that are grouped into blocks. Each block is cryptographically linked to the previous one after validation and undergoing a consensus decision." (Yaga et al., 2018) Thanks to encryption technologies, the single point of failure caused by an authorised third party has been overcome when it comes to verifying the authenticity of transactions.

The blockchain model leverages many features of the 'Peer2Peer' (P2P) model. This broker-free approach enables users to not incur avoidable costs related to third-party centralised authorisation operations. In this model, security standards are higher and transactions are committed faster as they are automatically accepted and saved by multiple agents. It makes it harder for hackers to exploit vulnerabilities of the system, thus reducing costs of security-related tasks. Furthermore, transactions can be easily made public and open access.

Figure 1 shows the basic components of the blockchain P2P architecture. There are many variations of this basic conceptual design, including other features, but the diagram is a useful way to describe the way blockchains work.

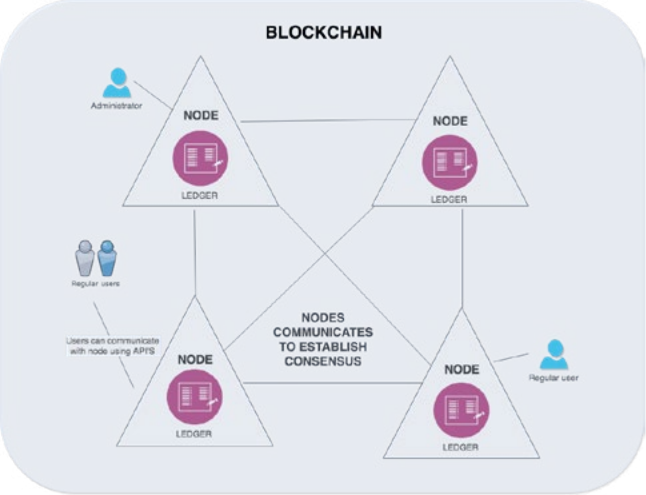


Figure 1. Blockchain distributed architecture

Hashes

Cryptographic hash functions are the main component of the blockchain model. These functions are widely utilised for several use cases, e.g. encrypting the data present in a block. Almost any input of any size (e.g., a picture or a text file) can be processed with the use of 'hashing'. The main goal of the hashing method is to compute a 'unique' static-sized output, i.e., a 'message digest'. Every single change in the input files may produce a totally different output message digest. Furthermore, two inputs cannot result in the same output (computationally), which means that hash algorithms are 'collision resistant' (second pre-image resistant).

The fast-computing SHA–256 algorithm (Secure Hash Algorithm with an output size of 256 bits) is a well-known and widely used algorithm supported by a majority of computing nodes and utilised by a lot of blockchain-based models. The NIST Secure Hashing website (Dang, 2014) contains FIPS specifications for all NIST-approved hashing algorithms. One of them, the SHA–256 algorithm, is specified in the Federal Information Processing Standard (FIPS) 180–4 (Dang, 2014).

Ledgers

Ledgers are composed of a set of transactions. Each *node* has a local copy of this set of transactions, i.e., the ledger. By the same token, a blockchain is usually composed of a set of *nodes*. The exchange of goods and services has been stored historically in analogue (pen-and-paper) ledgers. With the adoption of new computing paradigms, these analogue ledgers have been substituted with records in large centralised databases. These records are generated by a collection of users who entrust the operation of such databases to 'trusted' external agents, which actually own the data and ledgers. However, this centralized ledger approach has some disadvantages which include:

- The centralised agent is a single point of failure of the whole system. This means that at least the owner needs a backup system (or user) in case of loss or destruction.
- Each committed transaction should be validated by the central third-party agent. This means the validity of the transactions are only backed by the owner whom all users must trust.

- In the same way, all users must trust that this central agent corroborates the completeness of the ledger, since some transactions may be lost (purposefully or due to failures upon reception).

However, it should be noted that a vast majority of third-party 'trusted' agents and companies do backup transactions, which is in their best interest and the interest of their final users, validate the committed data, including all valid transactions.

Blocks

Each of the nodes in the blockchain may receive candidate transactions submitted by end-users. These transactions are then propagated to other nodes in the working group network. This operation, however, does not actually save the transaction in the blockchain. Subsequent to this process, mining nodes need to add the aforementioned transactions to the blockchain. Until then the committed transactions wait in the 'transaction pool' (a queue).

As mentioned before, the mining nodes are responsible for keeping the blockchain up-to-date by publishing freshly committed blocks. This process performs the actual operation of adding transactions to the blockchain. Thus, a 'block' is composed of validated transactions. To this end, the providers of transactions, who are shown in the input values of each transaction, must cryptographically sign the transaction to ensure its 'legitimacy', meaning that each of them had access to the appropriate private key. No blocks containing invalid transactions will be accepted in the blockchain. To this aim, the rest of the mining nodes in the network check the validity of each and every transaction in the published block. Once a block is created, it must be hashed. To this purpose, a 518 digest, which represents the block, will be created. The immutability of data is ensured by this method since even a change in a single bit of the block would drastically change the generated hash. In addition, a copy of the hash of every block is shared among all the nodes in order to improve security. This system prevents any change since every node can check if the hash matches.

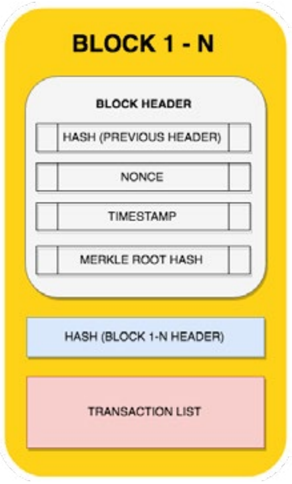


Figure 2. Block generic model

Each block typically consists of the following components:

- The block number, also known as 'block height'
- The current block hash value
- The previous block hash value
- The Merkle tree root hash
- A timestamp
- The size of the block
- A list of transactions within the block

The generated hash is stored in a data structure called 'Merkle tree' instead of the header of the block. The hash values of the gathered data are combined by the Merkle tree until there is a singular root, called 'Merkle tree root hash'. The presence of transactions within blocks and their summary can be efficiently verified by means of the aforementioned root. In addition, this data structure enables the system to detect any changes to the underlying data, therefore assuring that the data sent through the network is valid. Figure 3 shows an example of a Merkle tree:

- The bottom row shows the transaction data, i.e., the data to be summarised in the blockchain.
- The second row from the bottom represents the hashing process.
- The resulting hashed data is then combined and hashed. This is shown in the third row starting from the bottom.
- The top row represents the root hash, which hashes and combines H4 with H5. The root hash is created from the set of hashes containing all previous combinations and hashes.

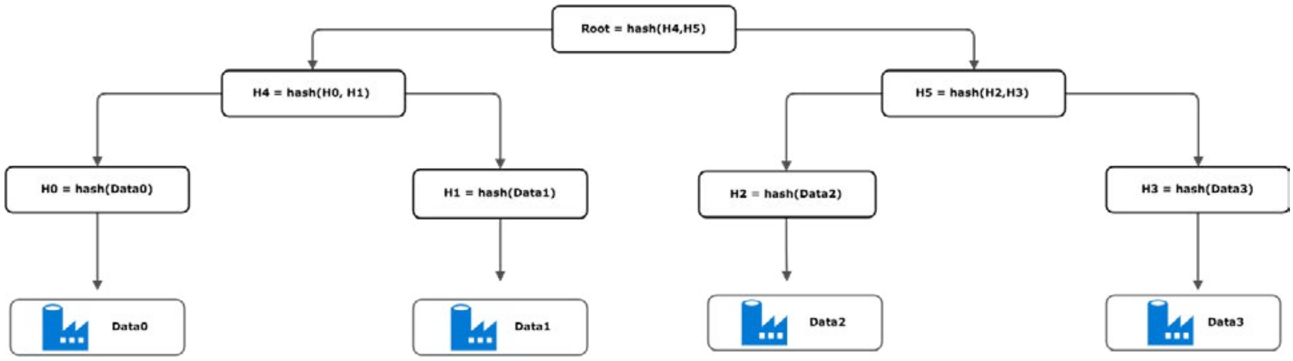


Figure 3. Merkle tree

Blockchain processes

In most blockchain platforms, the nodes of the blockchain network are owned by different organisations. The nodes may communicate with each other to agree on ledger content, and no central authority is required for both coordination and validation of all transactions.

Several algorithms have been proposed to solve the problem of reaching the agreement between nodes, i.e., the *consensus*. The blockchain receives transaction requests, which are submitted by users, to perform the operation it has been designed for. As a result of the execution of such a transaction, one or more ledgers store a record of the transaction which will never be modified or deleted. With this process, the *immutability* of the blockchain is achieved.

Blockchain security

Blockchain platforms are network environments where transaction data and parameters (value, state) are close to business logic. Blockchain transactions are mainly based on cryptographic and other mathematical models implemented for trading partners. The most popular cryptographic methodology used for blockchain transactions and data is asymmetric-key cryptography (Stallings, 1990) (also referred to as public/private-key cryptography). In this model, there is a pair of keys –a public key and a private key – used for signing the transactions and verifying the signatures in the following way (Bozic et al., 2016):

- Private key is used to generate transaction digital signatures.
- Public key is used to verify the signature generated with private key.

The public key may be made known to many users without affecting the security of the whole transaction. The private key, on the other hand, must be made known just to the key owner. Asymmetric cryptography guarantees that private key cannot be determined based on the knowledge of the public key.

Integration of blockchain with cloud environments

Cloud computing (Wang et al.) assembles large networks of virtualized services: hardware resources (CPU, storage, and network) and software resources (databases, message-queuing systems, monitoring systems, load-balancers). In the industry, these services are referred to as ‘Infrastructure as a Service’ (IaaS), ‘Platform as a Service (PaaS)’, and ‘Software as a Service’ (SaaS). Cloud computing services are hosted in large data centres, often referred to as ‘data farms’.

Based on resource and data management and the related security and privacy issue, we can distinguish three main types of cloud platforms: (i) public cloud, (ii) private cloud, and (ii) hybrid cloud. Public clouds offer unlimited access to shared data and resources for a wide group of users, but there is no guarantee that users’ data will be protected. Access to resources and data in private clouds is restricted and each user must be validated through strong authorisation and authentication procedures. Private cloud clusters are usually owned by enterprises and work under specific cloud standards. Hybrid clouds seem to be an ideal model of integration of the many private clouds into a joint global infrastructure. Such integration is done through the upper-level public layer. The main problem with that model is to reach an agreement among private cloud providers to work under a unified public cloud standard. Therefore, the 'many cloud model', where the distributed private cloud clusters are connected by using the standard P2P network (see Figure 4), is a much more realistic scenario.

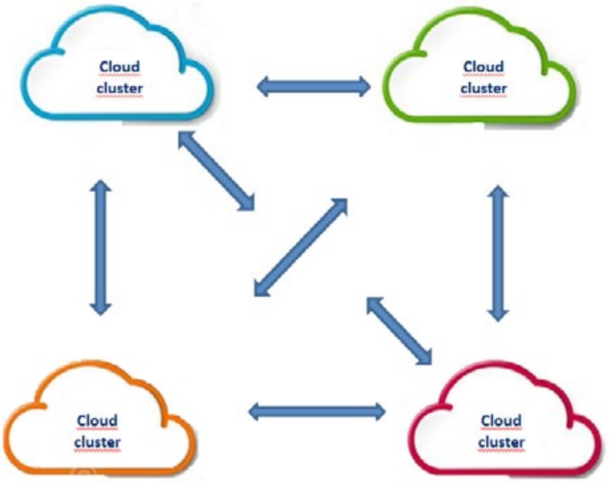


Figure 4. P2P-based 'Many clouds' architecture

It can be observed that a similar model works for the blockchain network, which was the first reason for trying to integrate both environments in order to improve the security policies in global clouds.

There are two main methods of integration of the cloud with blockchain platforms:

1. Using cloud for the development of blockchain applications and supporting the integration with enterprise networks (private clouds) to facilitate storage, replication and access to transactional data;
2. Using blockchain methods to improve the security of task, user and data management in the clouds.

Challenges, special conditions and main problems related to data and users' privacy, along with the recent ideas and developments are briefly discussed in the section below.

Cloud support for blockchain transactions and data – challenges and requirements

The number of transactions in blockchain networks can be enormous. The large volumes of generated data need scalable data processing services. Elasticity and scalability are some of the most important functionalities of the cloud systems to provide on-demand cloud resources for dynamically changing workload.

Public clouds can offer a large-scale network of resources available for the customers who pay only for the utilised ones. Private clouds usually need to be optimised for handling large data sets.

From the security perspective, cloud systems can effectively hide the physical location of data. Tuning activities can be carried out continuously with minimal impact on deployed applications, which is crucial for an efficient implementation of most of the blockchain algorithms. Any blockchain system must take into account data sovereignty rules and store and process data only in the locations permitted by the regulations. It means that the cloud service provider allows their customers to have control over the locations in which their data is stored and processed.

Another important issue regarding blockchain networks is system resilience and fault tolerance. It means that a failure of any single node in the blockchain network should not affect the work of the whole system. Cloud services help in such cases through the replication of data stored in data centres and the use of multiple software applications.

Finally, the implementation of blockchain algorithms in clouds may improve the security of the blockchain system itself. Software can be centrally maintained in a distributed cloud environment with data stored on a local data server. The recent examples of such successful integration of the blockchain with cloud platforms are Oracle Blockchain Cloud Service project (Oracle, 2017) and iEx.ec project (iEx.ec, 2018).

Blockchain support for the cloud users, task and data management – new ideas

The most recent technological developments and anonymization of the user's information and data in the cloud environments are inspired by blockchain technologies (Bozic et al., 2016). Blockchain seems to be a promising methodology for ensuring anonymity in large-scale clouds, an electronic wallet for user anonymity (Park and Park, 2017). Such an electronic wallet is installed when using blockchain technology, and after that it must be securely deleted from the system to avoid the private user's information being accessed by third parties.

Another new idea is to use blockchain proof of concept algorithms for secure data and task scheduling in the cloud. For example, the 'many clouds' model is used for illustrating the distributed P2P cloud cluster architecture. Each node in that P2P network corresponds to the cloud Service Provider (SP). The SP node may have a complex internal architecture: one SP node may be the master node for the local data and computational servers (slave nodes). The execution of the generated optimal schedule can be additionally monitored by the blockchain system in order to generate the recommendation list of the data storage servers, cloud services and cloud resource providers. This is totally new concept, which is currently one of our research tasks in our cloud development work.

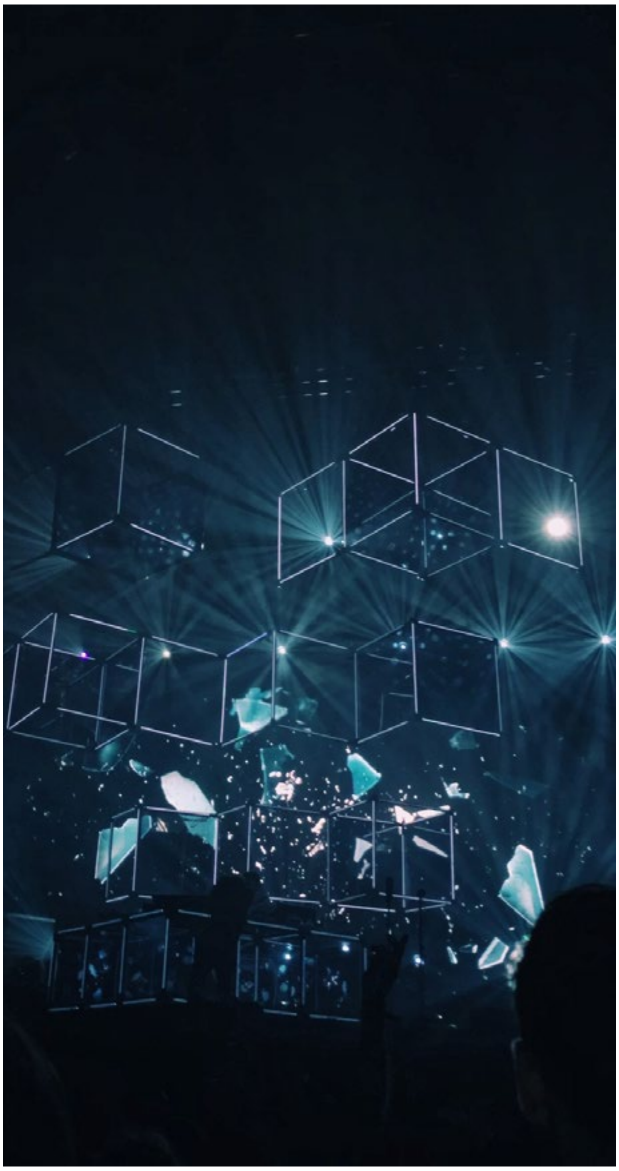
Conclusions

Blockchain is a popular financial technology, which uses ICT environments for virtual financial transactions using cryptocurrencies (e.g. Bitcoin). Blockchain customers store their transaction records in the blockchain P2P network, which effectively utilises the computing resources of its peers. A proof of work and a proof of stake are blockchain consensus algorithms that are used to improve the security of blockchain transactions.

In this paper, we briefly discussed the benefits of integrating the blockchain network with the elastic, scalable cloud environment in order to enhance the trustfulness of data servers and the security of data and user management. We also identified the challenges posed by this integration process. The new concept that we propose is to use blockchain algorithms for monitoring the execution of the security-aware task scheduling in the cloud, which is one of the most important research topic in today's cloud and fog computing. We believe that the new blockchain-based scheduling model will allow us to overcome the problem related to the implementation of the existing models in the real-life scenarios (Kołodziej et al., 2014).

Acknowledgement

This paper is based upon work done as part of COST Action IC1406 High-Performance Modelling and Simulation for Big Data Applications (cHiPSet), supported by COST (European Cooperation in Science and Technology). ■



REFERENCES

Il-Kwon, L. Young-Hyuk, K. Jae-Gwang, L. and Jae-Pil, L. (2014, June 30-July 3). The Analysis and Countermeasures on Security Breach of Bitcoin. *Proceedings of the International Conference on Computational Science and Its Applications.* Guimarães, Portugal. Springer International Publishing: Cham, Switzerland.

Christidis, K. and Michael, D. (2016). Blockchains and Smart Contracts for the Internet of Things. *IEEE Access, 4.* pp. 2292–2303.

Huh, S. Sangrae, C. and Soohyung, K. (2017, February). Managing IoT devices using blockchain platform. *Proceedings of the 2017 19th International Conference on Advanced Communication Technology (ICACT).* Bongpyeong, Korea. pp. 19–22.

Armknecht, F. Karame, G. Mandal, A. Youssef, F. and Zenner, E. (2015). Ripple: Overview and Outlook. In Trust and Trustworthy Computing. *Conti, M., Schunter, M., Askoxylakis, I., Eds.* Springer International Publishing, Cham, Switzerland. pp. 163–180.

Singh, S. Jeong, Y.-S. Park, J.H. (2016). A survey on cloud computing security: Issues, threats, and solutions. *J. Netw. Comput. Appl.* 75. pp. 200–222.

Dang Q. H. (2014). Secure Hash Standard. *Federal Inf. Process. Stds. (NIST FIPS) - 180-4.* Retrieved from https://www.nist.gov/publications/secure-hash-standard

CCAB. (2017). *Cloud Customer Architecture for Blockchain.* Cloud Standards Customer Council, http://www.cloud-council.org/deliverables/cloud-customer-architecture-for-blockchain.htm

Zeng, Z. Dai, H.-N. Xie, S. and Wang, H. (2017). An Overview of Blockchain Technology: Architecture, Consensus, and Future Trends. *Proc. Of the 2017 IEEE 6th International Congress on Big Data.* pp. 557-564.

Yaga, D. Mell, P. Roby, N. and Scarfone K. (2018). Blockchain Technology Overview. Draft NISTIR 8202. Retrieved from https://csrc.nist.gov/CSRC/media/Publications/nistir/8202/draft/documents/nistir8202-draft.pdf

Park J.H. and Park J.H. (2017). Blockchain Security in Cloud Computing: Use Cases, Challenges, and Solutions. *Symmetry.* 9(164). Retrieved from www.mdpi.com/2073-8994/9/8/164

Bozic, N. Guy, P. and Stefano, S. (2016). A tutorial on blockchain and applications to secure network control-planes. SCNS IEEE.

Oracle (2017). Oracle Blockchain Cloud Service project. Retrieved from https://cloud.oracle.com/blockchain

iEx.ec (2018). Retrieved from https://iex.ec/

Stallings, W. (1990). *Cryptography and Network Security: Principles and Practice.* Prentice Hall. p. 165.

EU DP (2018). 2018 reform of EU data protection rules, Retrieved from https://ec.europa.eu/commission/priorities/justice-and-fundamental-rights/data-protection/2018-reform-eu-data-protection-rules_en

Wang, L. Ranjan, R. Chen, J. and Benatallah B. (eds.) (2011). *Cloud computing: methodology, system, and application.*, CRC Press. Taylor & Francis.

Kolodziej, J. Khan, S.U. Wang, L, Kisiel-Dorohinicki, M. Madani, S.A, Niewiadomska-Szynkiewicz, E. Zomaya, A.Y. and Xu, C.-Z. (2014). *Security, energy, and performance-aware resource allocation mechanisms for computational grids.* Future Generation Comp. Syst. 31: 77-92

OPINION

CYBERSECURITY IN CRISIS

ADRIAN NEAL, MSC. SOFT. ENG. (OXON)
SENIOR FELLOW, OXFORD FOUNDATION FOR STRATEGIC CYBER DEFENCE

Adrian Neal is a graduate of the University of Oxford, holding a Master's degree in Software Engineering. His career in cybersecurity has spanned over 30 years, taking him from the City of London to Switzerland, New Zealand, Australia, the Netherlands, Luxembourg and finally back to Oxford. He has worked, at one time or another, in the banking, telecommunications, pharmaceuticals and airline industries, before returning to Oxford as the Founder and CEO of a university spin-out, Oxford BioChronometrics. Having had his research into Autonomous Malware Behaviour cited in both houses of the US Congress as well as the Financial Times, he also won the 2017 NATO Defence Innovation Challenge prize for advances in cybersecurity. He has now turned his attention to the application of communication theory and machine learning as a means to fundamentally change, once and for all, the way we detect malware. In 2018, he co-founded the public policy forum, the Oxford Foundation for Strategic Cyber Defence, as a catalyst for urgent policy changes to our national strategies for cybersecurity. Consequently, he remains Chief Scientist to a number of organisations that are dedicated to advancing this new approach to cybersecurity. He can be reached at adrian.neal@ofscd.org.

Introduction

Cybersecurity is in trouble; big trouble. When news broke in 2014 about the most successful cyber theft in history, the theft of Bitcoins valued at 400 million US dollars from the cryptocurrency vault of the Japanese Bitcoin exchange Mt. Gox ("Twice burned", 2017), the amount seemed staggering and the theft audacious. That was until 2016 and the attempted cyber theft of 1 billion US dollars from the account of Bangladesh Bank, held at the Federal Reserve Bank of New York ("Bangladesh Bank robbery", 2018). So when in January this year, a 532-million-US-dollar cyber theft from the cryptocurrency vault of another Japanese Bitcoin exchange, Coincheck ("The Coincheck hack", 2018) was announced, it seemed almost 'business as usual' by comparison. To paraphrase what CNN's Richard Quest said at the height of the 2009 financial crisis "A few billion here, a few billion there, and before you know it, you're talking real money."

However, a few weeks later, towards the end of February, things became much more serious. Reports were beginning to emerge of a cyberattack against the highly secure internal networks of the German defence and interior ministries, and that the attack was 'ongoing', having been first detected in late December of last year. To quote Deutsche Welle (2018, February 28) "The hackers reportedly infiltrated the government's IVBB (*Information Network Berlin-Bonn*) network, a specially designed communications platform which is separate from other public networks to ensure a supposed added layer of security (…) used exclusively by the chancellery, the German parliament, federal ministries, the Federal Audit Office and several security institutions in Berlin and Bonn; the former German capital where some ministries still have offices." Placing this into context, it also reported that the German government "receives roughly 20 attempted hacking attacks per day, while German intelligence services also carry out penetration tests once per week." Astonishingly, the malware had lain undisturbed on the IVBB network for up to a year.

According to anecdotal[1] reports being aired on German TV, the discovery of the malware was not from an alert generated by some advanced malware detection system but, rather disappointingly, from information passed to the government by the security services of a friendly foreign power. If this really was the case, then it was also the final nail in the coffin of any notion that our cyber defences are even remotely capable of defending against an attack on our national critical infrastructure or the most sensitive of our military networks. It should not be forgotten that NATO, of which the German ministry of defence would be a critical operational component, is only as strong as the (cyber) defences of its weakest member nation. Any penetration of the military networks of a single member nation may well allow access to shared NATO military networks, due to current network architectures that are based on the 'Trusted Network' axiom: "If you have authenticated access to network A, you are therefore trusted and thus granted access to networks B, C, D, etc.", a model commonly known as 'Federated Identity'. The paradox is, of course, that this model assumes that the network authentication process cannot be breached, except that we know that it can.

It should not be forgotten that NATO, of which the German ministry of defence would be a critical operational component, is only as strong as the (cyber) defences of its weakest member nation.

This attack, and the resulting picture that it paints of Western cyber defences, both militarily and civilian, raises some painful questions, such as what is wrong with our penetration tests if we fail to uncover, week after week, how this malware 'penetrated' our networks? We might also ask what is wrong with our malware and anomaly detection systems if malware can remain undetected for almost a year? Might there be more malware installed on this network that we a) do not yet know about and b) have no way of determining?

In fairness to the Germans, they are by no means alone in facing these problems, and have been unfortunate in receiving far more unwelcome publicity than most others have received. The problems facing us from this type of malware have existed for almost 20 years, but its use as a cyber-weapon has steadily been increasing, leading us to the present crisis, where every serious, high-value attack, deploys this most pernicious of malware – the Remote Access Trojan (RAT). But this increase is not for nothing; it is used as the attacker's weapon of choice, because it works!

Remote Access Trojans

Back in 2002, Roger Grimes of Microsoft posted on the TechNet forum that RATs "are designed specifically for stealth installation and operation. Typically, exploited users either download and execute the malicious programs or are tricked into clicking rogue email attachments." As late as 2017, IBM are pretty much describing the same situation with the caution that "Most Advanced Persistent Threat (APT) attacks take advantage of RAT technology for reconnaissance, bypassing strong authentication, spreading the infection, and accessing sensitive applications to exfiltrate data. RATs are commercially available (e.g. Poison Ivy, Dark Comet) and can be maliciously installed on endpoints using drive-by-download and spear-phishing tactics. Organizations should specifically address RATs in their enterprise defence strategy at the endpoint layer. The risk is especially high when RAT infection occurs, as the detection of RATs in run-time is extremely difficult to do."

So what makes them so dangerous? Essentially, if their delivery (or infection) mechanism is through Zero-Day Exploits (ZDE), there is little hope of endpoint anti-virus

[1] Based on my own research

software detecting them. Additionally, their use of polymorphism and open source tools with executable code, bypass signature-based anti-virus detection, allowing the RAT to add its self and all of its components onto the anti-virus 'trusted application' list. Polymorphism results in a different RAT signature for each attack, so that there is no previously known signature by which to detect, while open source tools and executable code will already be listed as trusted applications.

Because it is both difficult to detect as it infects a host system, and almost impossible to detect once it is installed and operational, its Time-to-Discovery (TtD) is very long. According to a 2017 blog by Chris Gerritz referencing a report by FireEye, the median time to discovery of an attack, within the EMEA region, was 469 days after the initial compromise, versus a global median time of 146 days. It would seem that the EMEA region has a particular problem in this area.

The median time to discovery of an attack, within the EMEA region, was 469 days after the initial compromise, versus a global median time of 146 days.

Consistent with the breach at the German ministries, discovery tends to occur from external third parties, giving rise to significant risk and liability. Verizon estimated that in 2017, over 87 percent of all reported breaches were made by external parties with only 8 percent occurring internally in an active manner ("Data Breach Investigations", 2017).

Lack of Situational Awareness

So, what is happening here? We have a situation where we are just not understanding the environment as it is, and placing heavy reliance on perimeter security. As Amit Yoran, President of RSA, wrote back in 2015 "A lack of situational awareness among many information security professionals is one of the most pressing vulnerabilities in US cyber defences. One way in which we see this manifest is the false sense of safety some information security professionals feel. There is too much blind faith in the firewalls and other solutions they have deployed. Perhaps motivated by industry hype, a need to check a box on a to-do list, or fear, prudent scepticism and logic are supplanted by urgency for action. Belief is placed in products without true understanding, accurate perception of circumstances, or discrimination. Basic due diligence – evaluations, reference checks, pilot projects – is often overlooked. This fosters complacency and leaves systems exposed (...) Information security investment on signature- and rule-based prevention technologies such as firewalls and anti-virus software has been disproportionately high compared with spending on solutions that can detect and respond to incursions (...) Higher fences and thicker walls appear formidable, but opponents can borrow under, vault over, and even go around them. Some even blend in with the crowd at check points and are allowed to pass." He concludes that ultimately "accepting risk in exchange for a false sense of security is a bad trade."

Higher fences and thicker walls appear formidable, but opponents can borrow under, vault over, and even go around them.

Lessons from Online Banking in Benelux

So where might we look for solutions? What successes have there been in the past? In 2012, some of the Benelux banks were (also) facing a cybersecurity crisis.[2] Online banking fraud had started to escalate from about 1 million euros per year in 2009 to over 2 million euros ***per week*** by 2012. In theory, certain banks faced an existential crisis within less than a year if both the rate of fraud continued on its current trajectory and the banks did nothing to counter it.

They say there is nothing quite like an existential crisis to wake people from their slumber, and the banks promptly woke up to the realisation that they would be out of business if they did not figure something out very, very quickly. From the perspective of the online fraud research teams at these banks, it was nothing short of a dream (or nightmare) come true; every idea, no matter how trivial or complex, was given a chance to be tested, and surprisingly, many of them, (including the comparative analysis of keyboard/mouse click count and timing averages together

[2] Based on my own research.

with page view timing averages, on a per-account basis) were far more successful than originally thought, even if sometimes the fraud-reduction was only temporary, but allowing the banks to buy precious time, while more long-term solutions were implemented.

They say there is nothing quite like an existential crisis to wake people from their slumber, and the banks promptly woke up to the realisation that they would be out of business if they did not figure something out very, very quickly.

Whilst some client-side technologies were permanently implemented, giving an early warning that the customer's device might be infected with malware, it was combined with an analysis of the basic properties of a transaction: who was sending what, to whom, when, and maybe why; a somewhat rudimentary application of Signals Analysis in Communication Theory (encapsulated in the properties of Source, Sender, Channel, Receiver, Destination, Message, Entropy and Feedback) (Shannon, 1948) (Turing, 1940).

However, knowledge of the beneficiary (the whom) has traditionally been difficult to obtain, with the account often being held at another bank. However, when the beneficiary account information was augmented in a decision between the regional banks to share between themselves basic account information, fraudulent transactions could no longer hide, having previously taken advantage of the fact that the bank was always working with limited information about where the funds were going to. A rather simple addition of information radically changed the landscape for online banking fraud.

Cybersecurity – a New Problem?

It is this principle of observation of the basic, but ***fundamental*** properties of communication that may be the key to solving a problem we have been grappling with since the beginning of the Internet age.

Because technology is ever changing, and yet the problem of the security of our communications persists despite such technological advances, we can conclude that it is not, *per se*, a technological problem, but a problem of communication security, requiring a more fundamental solution. We know this to be true because from historical records, this problem has been around for a long time, with well-documented examples reaching back as far as the Roman emperor Julius Caesar. Technology is merely the medium through which information is transmitted and retrieved, and with an explosion of information in 'the information age', it is not surprising that this very old problem should become more prevalent and fool many of us into thinking that this is a new problem. It is not. It is an ancient problem that is now experienced by entire societies (anyone with an online bank or Facebook account), rather than by single entities (emperors, kings, princes, governments, armies, etc.).

Technology is merely the medium through which information is transmitted and retrieved, and with an explosion of information in 'the information age', it is not surprising that this very old problem should become more prevalent and fool many of us into thinking that this is a new problem.

Fundamental Principles - A New Approach to Detection

The logic behind using communication theory as a more robust basis for malware detection is precisely because it encompasses a set of properties that are fundamental to malware, as opposed to malware's transient properties, such as the application or operating system environment for which it is targeted. This is evidenced in that, irrespective of the device or network that is compromised, any attack involves communication between the attack tools (the malware) and the attacker. Even in highly automated attacks where the malware must act autonomously, there remains initial communication in the mechanism of the delivery of the malware into the network or onto the device. Since such communication is almost certain to be disguised as background chatter or noise, isolating it as a malicious communication should be the primary goal of good malware detection.

This is generally considered to be non-trivial, and as such, existing malware detection solutions prefer detection methods that focus on the interactions of the malware with specific technology, such as how certain malware might interact with, for example, Google Chrome on an iPhone 7. This preference makes commercial sense, in that malware is almost entirely written to exploit a technical flaw in a specific piece of software, thus allowing detection to be narrowly focused. The problem, however, is that such solutions never last, because the technology moves on; it may be an effective point solution for now, but at a fundamental level, it solves nothing.

This is evidenced in that, irrespective of the device or network that is compromised, any attack involves communication between the attack tools (the malware) and the attacker. (...) Since such communication is almost certain to be disguised as background chatter or noise, isolating it as a malicious communication should be the primary goal of good malware detection.

OPEN SYSTEMS INTERCONNECTION MODEL

Layer		Protocol Data Unit	Function
Host	7. Application	Data	High-level Application Programming Interfaces (API), including resource sharing and remote file access.
	6. Presentation		Data translation between networking services and applications, including character encoding, compression, encryption, etc.
	5. Session		Communication session management; continuous information exchange; multiple back-and-forth transmissions between two nodes.
	4. Transport	Segment, Data	Reliable transmission of data segments between points on a network, including segmentation, acknowledgement and multiplexing.
Media	3. Network	Packet	Structuring and managing a multi-node network, including addressing, routing and traffic control.
	2. Data Link	Frame	Reliable transmission of data frames between two nodes connected by a physical layer.
	1. Physical	Symbol (Baud)	Transmission and reception of raw bit streams over a physical medium.

Table 1. The Open Systems Interconnection Model. Source: IEEE, 1980.

However, if we were to look at the communication behaviour of malware at sub-layer five of the OSI Network Classification model (Zimmermann, 1980), and apply communications theory, we avoid specific application technologies and are free to focus solely on the lower-level communication channels, such as layers two, three and four (the Data Link, Network and Transport layers respectively, with the exception of layer five if encryption is employed).

This is where our theory becomes a difficult problem; isolating the malware signal in the communication layers this far down the network stack requires that we solve the traffic-noise (or needle-in-the-haystack) problem. Even in low-bandwidth systems (megabit channels), the volumes of traffic can be huge, requiring the ability to find one or a small set of signals in volumes of 1011 or more. However, in reality, we would want to apply this to the Internet backbone or telco-grade channels to exploit its full potential (terabit+ channels), meaning we would need to deal with traffic volumes of 1014 at least.

Whilst, in our proposed model, any solution is not fundamentally a technical solution, it does rely on advances in machine learning and technical environments capable of processing terabyte & petabyte data sets in polynomial (or feasible) time, and it is these advances that, in part, make the application of communication theory to the problem of cybersecurity plausible.

We should note at this point that machine leaning is not a panacea for solving any problem thrown at it. It is equally as important to understand what type of problems it can solve, based upon the type of data available. The by-product of using data only from the lower levels of the communications channel is that there are far less data elements (and dimensions) to deal with, enabling the application of very efficient Nonlinear Dimensionality Reduction (NLDR) algorithms, so as to reduce the computational space, and thus achieving polynomial processing time, which up until quite recently was the main obstacle of applying communication theory to solve the problem of cybersecurity, at the fundamental level or otherwise.

Historical Evidence of Efficacy

Whilst there is significant evidence that our approach is both logical and technically feasible, we claim that ***only*** a fundamental approach to the cybersecurity detection problem will create and maintain a cybersecurity defence posture that is capable of both neutralising current attacks and mitigating future threats. But what justifies such a belief? We have solid examples from history regarding the approach taken to the attacks against both the Enigma machines during World War II and the subsequent cold-war Venona code break *(a one-time-pad encryption scheme used for Soviet espionage).*

Only a fundamental approach to the cybersecurity detection problem will create and maintain a cybersecurity defence posture that is capable of both neutralising current attacks and mitigating future threats.

It is little remembered that until mid-1939, the British were using linguists in their attempt to decrypt German Enigma messages and were not having much success. Even by the early 1930s, the Polish were already making significant advances in their attacks against Enigma, using their fundamental mathematical understanding of how Enigma encrypted its messages. Just before the war broke out, the Polish mathematicians Jerzy Różycki, Henryk Zygalski and Marian Rejewski, passed their knowledge to the British, who subsequently used this knowledge to develop their own 'bombe', as described to them by the Polish team, and with some improvements, made it capable of breaking the more complex wartime Enigma codes.

By developing a decryption mechanism based on the ***fundamental*** mathematical properties of Enigma given to them by the Polish, the British were able to read substantial quantities of messages transmitted by the Germans during World War II. Even when confronted with messages encrypted with Enigma machines having additional wheels *(Ger: Steckern)*, such as from the German Navy, the same fundamental mathematical properties still held ("History of the Enigma", 2012).

After the war, the new Soviet threat prompted the establishment of yet another secret programme to decrypt enemy communications called Venona ("The U.S. Army's Signal Intelligence Service", 2016). Because the Soviets used the one-time-pad method of encryption, based on the combined work of Miller, Vernam, Shannon and Kotelnikov over a 63-year period (1882–1945), it was deemed *(and in fact proven by Shannon in a still-classified paper)* to be, mathematically at least, unbreakable. This meant that the Venona programme returned to the pre-war Enigma model of cryptanalysis via linguistics and cryptographic implementation errors *(multiple use of one-time-pads, poor randomisation, etc.)*. While there were some significant successes, thanks to the brilliant linguist and cryptanalyst Meredith Gardner at the NSA, it was nothing compared to the Enigma code break, and resulted in the decryption of less than two percent of the collected traffic.

In Conclusion

It is evidently clear that where fundamental principles are used as the primary means of attack, there is both immediate and long-term success. Conversely, where transient properties are used instead, success is minimal, at best.

We saw from the Benelux banking cybersecurity crisis that tackling cybersecurity from a non-technological perspective gave them the enduring breakthrough in defeating online banking fraud. Anecdotal evidence suggests that, six years later, there remains almost negligible fraud from malware at most of these banks as a result.

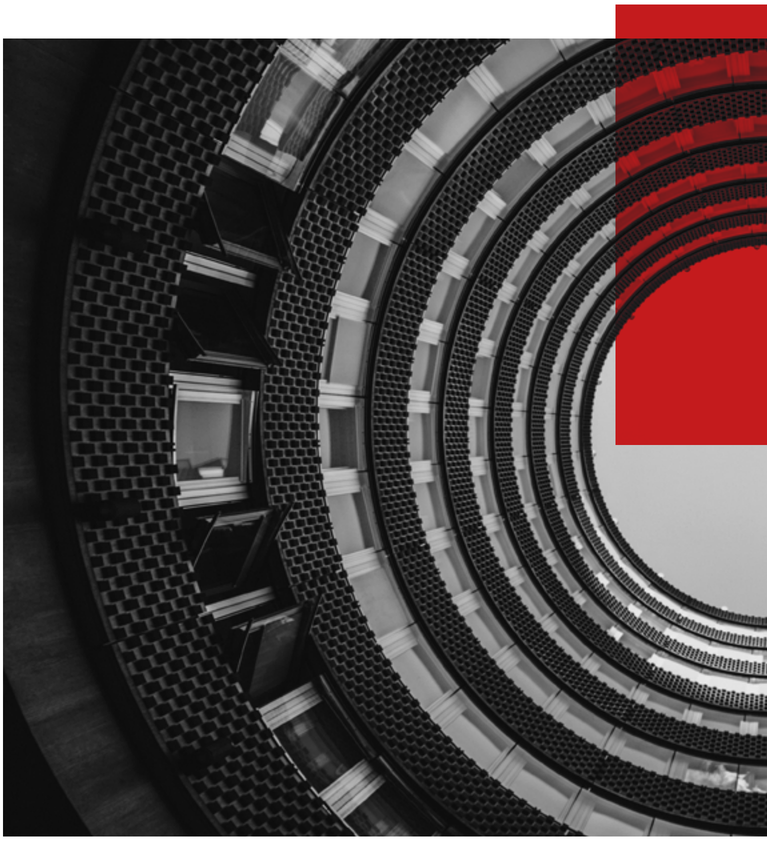
Clearly, there is a stark contrast in the level of malware detection successes between technological solutions and non-technical solutions, while this contrast was similarly apparent in the levels of success in the decryption of enemy messages between transient linguist methods of attack and a fundamental mathematical approach.

> ***It is evidently clear that where fundamental principles are used as the primary means of attack, there is both immediate and long-term success. Conversely, where transient properties are used instead, success is minimal, at best.***

The evidence speaks for itself. Like the effect the discovery of penicillin had on medicine, the cybersecurity crisis could be resolved if a new approach was taken by both governments and major enterprises. Moving detection to the lower network levels, and applying machine learning with communication theory, would mean that entire regions, perhaps even countries, could be protected from an attack with, comparatively, minimal effort and cost, especially if applied to the Internet-backbone.

It is no secret that we have not been winning the cybersecurity war for some time and are now at a crossroads; with advances in artificial intelligence (AI) offering us both future benefits and threats, it is quite clear that we ought not to proceed any further with AI until we have solved, once and for all, the current cybersecurity crisis. Being unprepared for an AI-driven, exponentially advancing cyberwar, we stand to permanently lose the only remaining chance we have to match our cyber defences to the approaching threat, and that will have far reaching and untold consequences.

We cannot let this happen. ■



REFERENCES

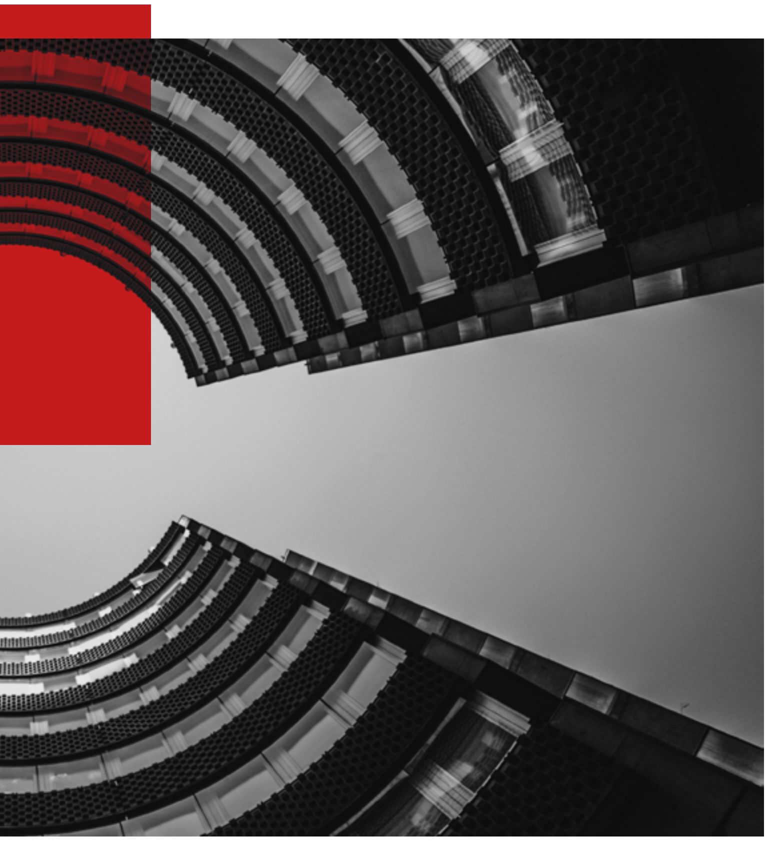
Twice burned - How Mt. Gox's bitcoin customers could lose again. (2017, November 16). Retrieved from https://www.reuters.com/investigates/special-report/bitcoin-gox/

Bangladesh Bank robbery. (2018, June 11) Retrieved from https://en.wikipedia.org/wiki/Bangladesh_Bank_robbery

The Coincheck hack and the issue with crypto assets on centralized exchanges. (2018, January 29). Retrieved from https://www.reuters.com/article/us-japan-cryptocurrency-q-a/the-coincheck-hack-and-the-issue-with-crypto-assets-on-centralized-exchanges-idUSKBN1FI0K4

Quest, Richard (2009) Quest means Business. Cable News Network.

Germany admits hackers infiltrated federal ministries, Russian group suspected. (2018, February 28). Retrieved from http://p.dw.com/p/2tTrh



Gerritz, CBreach Detection by the Numbers: Days, Weeks or Years? (2016, July 27). Retrieved from https://www.infocyte.com/blog/2016/7/26/how-many-days-does-it-take-to-discover-a-breach-the-answer-may-shock-you

IBM. Malicious Software for Endpoint Takeover and Exploitation. Retrieved from http://www.trusteer.com/en/glossary/remote-access-trojan-rat

Grimes, R. Danger: Remote Access Trojans. (2002, September). Retrieved from https://technet.microsoft.com/en-gb/library/dd632947.aspx

Yoran, A. & Robertson W. (2015) Failures of the Security Industry. RSA White Paper. Retrieved from https://www.emc.com/collateral/white-paper/h14039-failures-of-the-security-industry.pdf

Verizon. (2017) Data Breach Investigations Report. Retrieved from https://www.ictsecuritymagazine.com/wp-content/uploads/2017-Data-Breach-Investigations-Report.pdf

Shannon, Claude Elwood (1948). A Mathematical Theory of Communication. The Bell System Technical Journal.

Turing, Alan (1940), Erskine, Ralph; Marks, Philip; Weierud, Frode, eds., Turing's Treatise on Enigma (The Prof's Book).

Zimmermann, Hubert (1980). OSI Reference Model - The ISO Model of Architecture for Open Systems Interconnection". IEEE Transactions on Communications.

History of the Enigma. Retrieved from http://www.cryptomuseum.com/crypto/enigma/hist.htm

The U.S. Army's Signal Intelligence Service. Retrieved from https://www.nsa.gov/news-features/declassified-documents/venona/

POLICY REVIEW

PROTECTION OF INTELLECTUAL PROPERTY IN CYBERSPACE UNDER INTERNATIONAL HUMANITARIAN LAW

JOOST BUNK

(1990) holds a LLM Public International Law from Leiden University and is currently pursuing a LLM IT Law at Groningen University. While written in a personal capacity, Joost Bunk is currently a Policy Officer at the Task Force International Cyber Policies at the Netherlands Ministry of Foreign Affairs.
The article is based Bunk's thesis, which he wrote for Leiden University in the course of a research internship at the Cyber Operations and Cyber Security Department of the Netherlands Defence Academy. The author wants to express his gratitude to the Netherlands Defence Academy, especially Prof. P.A.L. Ducheine and to Leiden University, especially Dr. R.W. Heinsch, for enabling this unique and interesting opportunity. The thesis was awarded runner-up in the 2017 Junior Scholar Award competition of the International Conference on Cyber Conflict (CyCon) of NATO's Cooperative Cyber Defence Centre of Excellence.

Introduction

States and regional security organisations are at an ever-increasing pace, developing cybersecurity strategies and introducing offensive cyber operations in the military. These developments raise a question as to how international humanitarian law can regulate these cyber operations.

This aforementioned question is the focus of this article: the protection of intellectual property in cyberspace under international humanitarian law. Intellectual property can be defined as a novel product of human intellectual endeavour (Macqueen, Waelde, and Laurie, 2007, p. 7). Intellectual property rights, copyrights, patents and trademarks protect intangibles, a concept which gives rise to a great variety of challenging questions regarding domestic law, human rights law and international humanitarian law.

Modern day information societies are digitalising continuously and the production of intellectual property is becoming increasingly important for their economic sustenance. Equally, there is an increasing number of cyber operations leading to an ever-growing interest in developing cyber capabilities. Former Director of the U.S. Cyber Command General Keith B. Alexander characterised cyber operations designed to gain access to the intellectual property of American corporations as the "greatest transfer of wealth in human history" (Miles, 2011). Cyberspace as an operational domain or a battlefield encompasses a very different territory than its conventional counterparts. This means that any network, computer, router, server or mobile satellite command station is potentially part of the domain. The economic importance of intellectual property and the rising use of cyber operations by malicious actors, combined with the ongoing digitisation of both production and storage of intellectual property and the characteristics of cyberspace make intellectual property a valuable target for cyber operations.

International humanitarian law, however, lacks specific provisions on intellectual property. The absence of precise regulations, the interest in intellectual property as a target and the rise of cyber operations, make the protection of intellectual property under international humanitarian law a very valid question. The research question of this paper is aimed at exploring the extent of protection that international humanitarian law currently provides to intellectual property in cyberspace concerning cyber operations in the context of an armed conflict or occupation. For this purpose, the development of the protection of property and intellectual property under international humanitarian law will be discussed. To provide a comprehensive answer to the research question, the protection of intellectual property under the rules of belligerent occupation will also be addressed.

The Protection of Intellectual Property under International Humanitarian Law

Since it is clear from the start that there are no specific rules on the protection of intellectual property under international humanitarian law, the possible protection of intellectual property through the already existing 'normal' property law will be explored. In order to achieve this, the concept and the development of the protection of property under the various instruments of international humanitarian law will be discussed first. Following this, the scarce coverage of intellectual property in international humanitarian law will be discussed. But first, since intellectual property law and international humanitarian law are the fields of law that do not often meet, the section below will start with a 'crash course' in intellectual property law.

The intangible concept

For over one hundred and fifty years, the term 'intellectual property' has been used to refer to the general area of law that encompasses copyrights, patents, trademarks and as well as a host of other related rights for objects such as databases and software (Bently and Sherman, 2008, p. 7). Intellectual property law regulates the creation, use and exploitation of mental or creative labour. Intellectual property is, as pointed out previously, a novel product of human intellectual endeavour. Therefore, intellectual property rights protect intangibles, which gives rise to questions over the control of the property and its protection (Macqueen et al., 2007, p. 7). The use of the term 'property' implies the existence of rights and remedies in respect of the property and unwarranted interference with it. Furthermore, the use of the term also implies a system of control to be exercised by the right holder. Intellectual property rights are concerned with identifying and policing permissible and impermissible acts with regard to intellectual production and are therefore relatively comparable to tangible property. However, all forms of intellectual property must qualify for protection according to stringent criteria that vary depending on which kind of intellectual property right is being sought. For example, creative labour can be protected by a copyright if this intellectual endeavour is sufficiently original according to the relevant legislation (Van der Kooij, 2015, p. 91). It is important to note that it is not the eventual produce of this endeavour, but the intellectual labour that is protected. A statue, a photograph or a painting can be protected if it is original; however, this does not mean that the said statue, photograph or painting is protected by a copyright.

The fact that intellectual property rights are separate from the objects in which they are embodied may be perceived as counter-intuitive (Bently and Sherman, 2008, p. 2). This idea is further complicated by the fact that intellectual property rights, as rights over intangibles, limit what owners of movable property are able to do with things they own (Macqueen et al., 2007, p. 7). The owner of Frits Kalshoven's *Constraints on the Waging of War* is, as the owner of the book, entitled to do with a copy of it as one pleases, except for the activities which are reserved to Frits Kalshoven as the copyright holder, which include, inter alia, copying and spreading of self-produced copies. Destroying or damaging a copy, if one ever would, is not prohibited under intellectual property law.

For the purpose of this research, it is important to note that there are three notions involved when it comes to intellectual property. The first notion is intellectual property, the intellectual labour which is the intangible concept of a creative work. Second, this intangible concept is only protected when it manifests itself in a physical form, a statue or a digital picture, and goes beyond existing solely in the mind of the creator (Van der Kooij, 2015, p. 91). Last, depending on the respective intellectual property law, the creator is given certain intellectual property rights. These rights are possessions and as such can be transferred to others (Van der Kooij, 2015, p. 105).

The so-called 'propertisation' of intellectual property renders the already complex field of intellectual property law even more complicated (Carrier, 2004, p. 4). There is a growing tendency for human rights courts and human rights treaties to recognise that intellectual property should be afforded the same protection as tangible property (Hansen, 2008, p. 434). This acknowledgment was already present in the Universal Declaration of Human Rights of 1948 (Van der Kooij, 2015, p. 21). In Article 27(2), the Declaration states: "Everyone has the right to the protection of the moral and material interests resulting from any scientific, literary or artistic production of which he is the author." The ECtHR stated in *Anheuser Inc. v Portugal* that "intellectual property incontestably enjoys the protection of Article 1 of Additional Protocol No.1 ECHR (*Anheuser-Busch Inc. v. Portugal*, 2007). With regard to this, it is interesting to note that the French version of Article 1 of Additional Protocol No. 1 uses the term 'biens' while the English version uses 'possessions', a definition and a translation point also raised by Macak hereafter.

These findings resulted in an extensive academic debate whose effects have not yet crystalised completely (Helfer, 2009, p. 52). However, it can be argued that a consensus exists that when discussing intellectual property as 'normal' property, neither the abstract intellectual production nor the product itself is meant, but the intellectual property right attached to it (Geiger, 2009, p. 117). In other words, the intellectual property right deserves the same protection as other property. Interestingly, while intellectual property rights play an important role in the development of digital technologies, thereby shaping the nature of cyberspace, cyberspace in return creates a threat to intellectual property rights (Rahmatian, 2015, p. 93). The speed of information exchange in cyberspace, the protected works accessible online and a relatively easy way of violating intellectual property rights by e.g. copying have resulted in a rampant violation of intellectual property (Somu, 2006, p. 62).

Interestingly, while intellectual property rights play an important role in the development of digital technologies, thereby shaping the nature of cyberspace, cyberspace in return creates a threat to intellectual property rights.

The author is well aware of the fact that terms, norms and principles found in domestic law, intellectual property law and human rights law cannot be implemented in international humanitarian law without paying due regard to the context.

Winding roads: from civilian property to civilian objects

International humanitarian law has protected civilian property for almost as long – and for the same reasons – as it has protected civilian persons (Brilmayer, 2008, p. 418). This protection of property can be considered customary international law (Biehler, 2007, p. 432).

The unprecedented suffering and destruction caused by World War II spurred the establishment of new international law conventions, including one aimed at protecting civilians (Pictet, 1951, p. 473). Geneva Convention IV was the first international instrument to specifically protect civilians (Brilmayer, 2008, p. 421). Civilian property protections appear in several different sections of Geneva Convention IV. Article 33 of Geneva Convention IV establishes a general prohibition on pillaging. It also guarantees for all types of property, whether belonging to private persons, local communities, or national governments (Brilmayer, 2008, p. 422). Article 53 of Geneva Convention IV concerning private property under enemy occupation, is even more specific: "Any destruction by the Occupying Power of real or personal property belonging individually or collectively to private persons [...] is prohibited."

Earlier codifications such as the Lieber Code and the Hague Regulations safeguarded property because property was seen as essential in mitigating civilian suffering during wartime. The U.S. delegate at the Diplomatic Conference stated that these provisions were enacted "in order to spare civilian populations the sufferings which might result from the destruction of their houses, clothes, foodstuffs and the means of earning their living [...]." (Geneva Convention Final Record Vol. II-A, 1949, p. 649). In the official commentary, it was further mentioned that "the purpose of this Convention is to protect human beings, but it also contains certain provisions concerning property, designed to spare people the suffering resulting from the destruction of their immovable and movable property (houses, deeds, bonds, etc., furniture, clothing, provisions, tools, etc.)" (ICRC, 1958, p. 226).

Between 1974 and 1977, the two Additional Protocols to the Geneva Conventions were drafted; their purpose was to modernise the Geneva Conventions and correct certain gaps and imperfections that had been exposed in the intervening years. These Additional Protocols expand on Geneva Convention IV's valuation of property when mitigating civilian suffering (Brilmayer, 2008, p. 427). Article 52 of Additional Protocol I introduces and defines the term 'civilian objects' and prohibits attacks against civilian objects during all periods of an international armed conflict, not just during an occupation. It defines civilian objects *a contrario* to include all objects that are not military objectives. Lastly, it introduces a clause to provide guidelines for situations in which the nature of the object is in doubt (Dinstein, 2010, p. 91).

Additional Protocol I notably departs from the use of the word 'property' and introduces a broader term – 'civilian object' (Brilmayer, 2008, p. 428). The term 'civilian object' was introduced to circumvent the discussion that arose between the Soviet Union and China *versus* the U.S., Canada and the United Kingdom in drafting the Geneva Conventions. The socialist countries contended that civilians not only relied on civilian property for sustenance, but in their case also on public-owned property. The U.S., Canada and the United Kingdom objected to the Soviet proposal as it would overextend the protection of state-owned property, for which there is no basis in international law (Brilmayer, 2008, p. 426).

While the introduction of this term circumvented the discussion, it also introduced a new term of which the exact definition is unclear. On the definition of the term 'object', the 1987 Commentary states: "The English text uses the word 'objects', which means 'something placed before the eyes, or presented to the sight or other sense, an individual thing seen, or perceived, or that may be seen or perceived; a material thing.'" (ICRC, 1987, Art. 52). The Commentary continues: "The French text uses the word '*biens*', which means '*chose tangible, susceptible d'appropriation*'" (ICRC, 1987, Art. 52). The 1987 Commentary concludes that it is clear that in both English and French the word means something that is visible and tangible (ICRC, 1987, Art. 52). The scope of the term 'civilian object' is broad enough to encompass the term 'property' found in earlier international humanitarian law instruments. Any discussion of civilian objects can, therefore, be assumed to include private property consisting of immovable or movable property, provided they are visible and tangible.

This contention that the term 'civilian object' is inclusive of civilian property is also supported by the structure of the third chapter 'Civilian Objects' of Additional Protocol I in which Article 52 is located. The latter opens the chapter 'General Protection of Civilian Objects' and subsequently lays out more detailed protection regimes for specific kinds of objects. Article 53 details the protection of cultural objects and places of worship, and mentions both immovable and movable property. Article 54 then goes on to cover 'The Protection of Objects Indispensable to the Survival of the Civilian Population' and has specific rules for the protection of both personal (such as foodstuffs) and real (such as drinking water installation) property. Article 56 regards 'The Protection of Works and Installations Containing Dangerous Forces' and focuses solely on immovable property. It can be concluded that movable property is included under protection for civilian objects, as long as it is not being used by the military and as long as this property is visible and tangible.

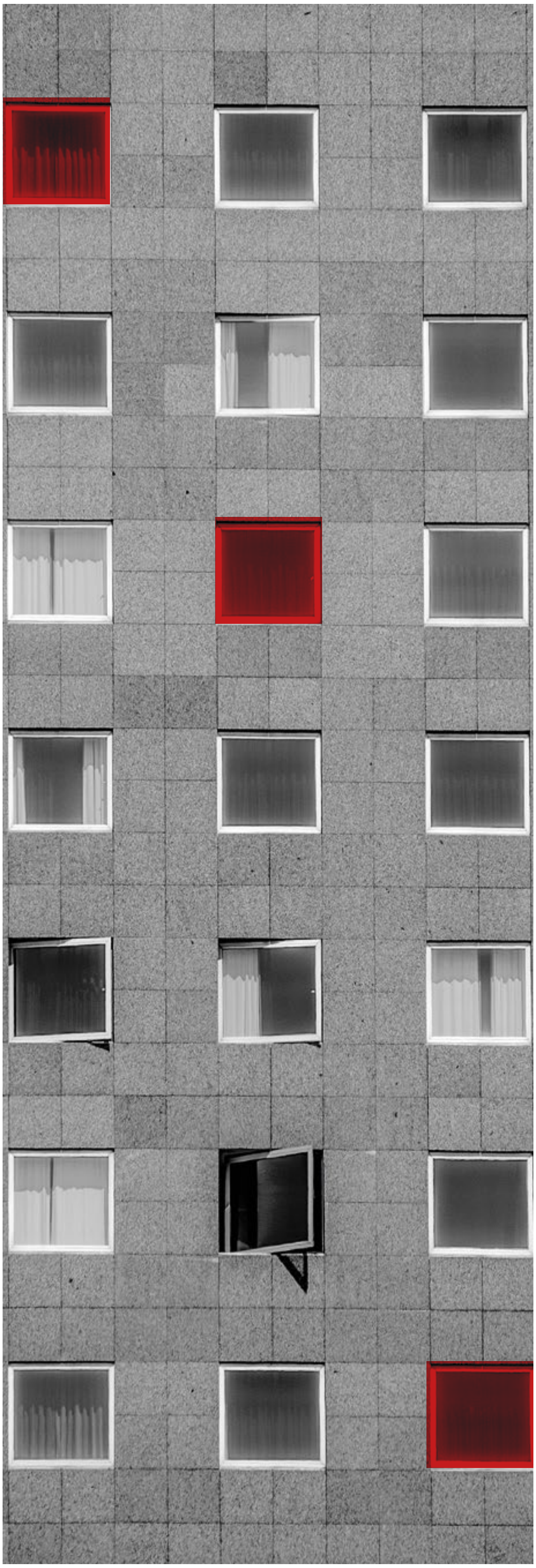
Rule 100 of the Tallinn Manual 2.0 closely follows Additional Protocol I but adds a specific dimension to cyber operations: "[...] Military objectives may include cyber infrastructure." With regard to civilian objects, the Experts note: "The meaning of the term 'object' is essential to understanding this and other Rules found in the Manual. An 'object' is characterized in the Commentary as something 'visible and tangible'. This usage is not to be confused with the meaning ascribed to the term in the field of computer science, which connotes entities that can be manipulated by the commands of a programming language. For the purpose of this Manual, computers, computer networks, and other tangible components of cyber infrastructure constitute objects" (Tallinn Manual 2.0, Rule 100, Comment 2).

Both Dinniss and Macak disagree with the strict approach of the Experts. Macak (2015, p. 20) points out that in francophone legal literature the French word 'bien' is not limited to just objects which have a physical presence in the real world, but is divided into tangible and intangible sub-categories in French speaking jurisdictions. Dinniss (as cited in Brilmayer, 2008, p. 443) argues that the 1987 Commentary fails to take into account discussions of working committees or the Diplomatic conference on this topic. Dinniss argues that it is clear from the 1987 Commentary that the definitional discussion about the term 'object' was originally launched to distinguish the term as a 'thing' from an 'aim or purpose' (a military operation), rather than to exclude intangible objects from the definition. Therefore, based on these two arguments, intangible and tangible civilian objects should be afforded equal protection.

Not fully caught up: international humanitarian law and intellectual property

According to Livojia and McCormack (2012, p. 53), the Tallinn Manual fails to take the destruction of data and the value of digital assets sufficiently seriously. They argue that this failure is to a large extent reflective of the current conceptual framework of international humanitarian law, which has not caught up with the recent development of the concepts of intellectual property and intangible assets. While threats to intellectual property are often less visible than threats to critical infrastructure, they may be the most pervasive cyberthreat extant (U.S. Department of Defense, 2011, p. 4).

In the light of this, it is most surprising that in 1948, the Nuremberg Trials did touch upon intangible property in the I.G. Farben Trial and in the Krupp Trial. These two trials



were part of the twelve subsequent Nuremburg Trials held by the American Military Tribunal following World War II. The American Military Tribunal, while discussing property in the Krupp Trial, found that "Property offences recognized by modern international law are not, however, limited to physical tangible possessions or to open robbery in the old sense of pillage, but include the acquisition of intangible property and the securing of ownership, use or control of all kinds of property by many ways other than open violence" (*USA v Krupp*, 1948, p.129). In this judgment, the Tribunal also held that respect for private property under Article 46 of the Hague Regulations does not mean merely protection from loss of ownership: for a breach to occur, it is enough if the owner is actually prevented from exercising his rightful prerogatives (*USA v Krupp*, 1948, pp. 137–8).

The Tribunal subsequently held the following in the I.G. Farben Trial: "In our view the offences against property defined in the Hague Regulations are broad in their phraseology and do not admit any distinction between 'plunder' in the restricted sense of acquisition of physical properties, […] the plunder and spoliation resulting from acquisition of intangible property such as is involved in the acquisition of stock ownership, or of acquisition of ownership or control through any other means." (*USA v Krauch*, 1948, p. 46). Even though not explicitly mentioned by the Military Tribunals, according to Dinstein (2009, p. 225), the protection of intangible assets is also where intellectual property comes into the fold.

As mentioned previously, the Tribunal particularly discussed the property offences found in Articles 46, 47, 52 and 53 of the Hague Regulations (*USA v Krauch*, 1948, p.46). However, the phraseology in both trials is broad and does not specify the mentioned provisions: 'Property offences recognized by modern international law' and 'the offences against property defined in the Hague Regulations'. Based on this, it could be argued that this interpretation is not solely limited to Article 46, 47, 52, and 53, but it potentially includes Article 56 and Article 23(g) of the Hague Regulations as well.

Article 46 of the Hague Regulations is similar to Article 53 of Geneva Convention IV. The 1958 Commentary states the following about the relationship between those Articles: "In the very wide sense in which the Article must be understood, the prohibition covers the destruction of all property (real or personal), whether it is the private property […], State property, […]. The extension of protection to public property and to goods owned collectively reinforces the rule already laid down in the Hague Regulations, Article 46 and Article 56, according to which private property and the property of municipalities […] must be respected" (ICRC, 1958, Art. 53, p. 302). Subsequently, the Commentary continues: "The prohibition of destruction contained in the present Article may be compared with the prohibition of pillage and reprisals in Article 33 of Geneva Convention IV" (ICRC, 1958, Art. 53, p. 302). Based on the foregoing, it could be argued that the Krupp/I.G. Farben Trials' interpretation of property in the provisions covering property offences could also be applied to similar and successor provisions found in the Geneva Conventions. Furthermore, the reference to Article 33 of Geneva Convention IV brings this interpretation outside the limited occupation paradigm, since Article 46 and Article 53 of the Hague Regulations are only applicable during occupation.

Therefore, based on the use of a similar language in the Geneva Conventions and the Hague Regulations, the intention to reinforce both the rules laid down in the Hague Regulations through Geneva Convention IV and the equalisation of rules on property offences in and outside occupation, it could be argued that intellectual property rights are protected under all property offences related provisions in the Geneva Conventions as well. Furthermore, while the Krupp/I.G. Farben Trials predate the Geneva Conventions, it could be argued, based on the foregoing, that the interpretation found in these Trials is equally applicable to the provisions found in Geneva Convention IV.

In the previous paragraph, it was established that Additional Protocol I abandons the use of the word 'property' and instead introduces the term 'civilian object'. Furthermore, it was found that, in principle, the term 'civilian object' is broad enough to encompass both immovable and movable property, provided that the object is tangible and visible. This strict interpretation, which excludes non-visible and non-tangible objects from the protection that Additional Protocol I provides, appears to be an anomaly.

The strict tangibility requirement results in intellectual property created in cyberspace qualifying as intangible and therefore not being a 'civilian object' in all three forms: the intellectual labour per definition, the digital product and the intellectual property right (intangible possession). The result of the strict interpretation of 'civilian objects' is that everything outside its scope of application is not afforded the protection provided for under the principles and rules with regard to the conduct of hostilities in Additional Protocol I (Schmitt, 2015, p. 97). The result of this exemplifies how the tangibility requirement is an anomaly in the development of international humanitarian law. Intellectual property is afforded protection in relation to property offences; however, by not fulfilling the tangibility requirement, it can be the object of an attack and the possible destruction of it does not have to be taken into account. In other words, intellectual property is protected under the provisions relating to property offences, but it is outside the protective measures against targeting because it lacks the tangibility and visibility requirement. It seems, therefore, that in the body of rules of international humanitarian law there is a disparity in protection within the property offences paradigm and the targeting paradigm, each providing a different level of protection for intellectual property. The full extent of these implications will be discussed in the following chapter.

Intellectual property is protected under the provisions relating to property offences, but it is outside the protective measures against targeting because it lacks the tangibility and visibility requirement.

The Tallinn Manual 2.0 follows the tangibility requirement and does not provide guidance on intellectual property and does not mention it either in relation to civilian objects or, by reference, to the Nuremberg Trials. However, intellectual property is briefly touched upon by the Experts in their discussion of cultural property. Rule 142 of the Tallinn Manual 2.0 governing the Respect and Protection of Cultural Property' states that "The parties to an armed conflict must respect and protect cultural property that may be affected by cyber-operations or that is located in cyberspace. In particular, they are prohibited from using digital cultural property for military purposes."

This rule is derived from the 1954 Hague Cultural Property Convention and its 1954 and 1999 Protocols. Article 1 of this Convention states that "the term 'cultural property' shall cover, irrespective of origin or ownership: *(a)* movable or immovable property of great importance to the cultural heritage of every people, [...] (Hague Cultural Property Convention, 1954, Art. 1). This protection and definition (Tallinn Manual 2.0, Rule 142, Comment 2) of cultural property applies to international armed conflict (Additional Protocol I, Art. 53) and can be considered customary international law (ICRC, 2005, Rule 38).

Comment 4 to Rule 142 of the Tallinn Manual 2.0, which is based on Article 53 of Additional Protocol I (Tallinn Manual 2.0, Rule 142, Comment 1, no. 1320), states that "The Experts considered whether intangible items could qualify as 'property' for law of armed conflict purposes." Based on the Krupp/I.G. Farben Trials, one could say that intangibles can indeed qualify as property. However, Comment 4 continues that "Recall that in the context of civilian objects, as that term is used in Article 52 of Additional Protocol I, the Experts generally rejected characterization of intangible items such as data as an 'object'". This finding is analogous to their findings with regard to other civilian objects. While the Hague Cultural Property Convention predates Additional Protocol I by almost 25 years, the Experts interpret the term 'property' according to the tangibility requirement found in Additional Protocol I, therefore excluding intangible property. Following Dinniss, however, and based on the Krupp/I.G. Farben Trials, property under the Hague Cultural Property Convention could also encompass intangibles (Harrison Dinniss, 2014, p. 263).

According to Comment 5, "Other Experts emphasized that the term 'property' is not always limited to tangible objects. An example of a notion of intangible property that is well accepted in international law and that appears in most domestic legal systems is intellectual property." This minority of Experts comes to a conclusion analogous to the finding of the Krupp/I.G. Farben Trials. Both refer to the already existing protection of intangibles in other legal systems. If the interpretation of this minority of Experts would be followed, intellectual property, provided it also qualifies as cultural property, would be afforded protection in the targeting paradigm. This is not in line with the strict interpretation of civilian object as seen above. The examples provided by these Experts to support their position include objects that are created and stored on a computing device and therefore only exist in a digital form, such as musical scores and digital films (Tallinn Manual 2.0, Rule 142, Comment 5). Since they only exist in a digital form, they would qualify as intangibles and are, by the same token, not subject to protection. It seems that the line of argumentation here is that certain intangibles are protected, provided they qualify as cultural property, thus making an exception to the strict rule of intangibly.

While the Experts are right by referring to intellectual property law as a mechanism to protect intangibles, the protection that intellectual property law provides for these intangibles is neither based on the cultural qualification nor it protects against destruction of an object. The fact that the reference to intellectual property law to provide an argument for the protection of cultural intangibles is not so well suited is also evident in Comment 6 in which none of the Experts takes the position that not all digital manifestations of cultural property are entitled to the protection under this Rule (Tallinn Manual 2.0, Rule 142, Comment 6). The Experts applied protection only to digital entities where the physical original is either inaccessible or has been destroyed, and where the number of digital copies that can be made is limited. By contrast, intellectual property law provides protection for intellectual labour provided it is original and embodied in a product, the protection is not dependent on the scarcity or inaccessibility of these products.

While the Experts are right by referring to intellectual property law as a mechanism to protect intangibles, the protection that intellectual property law provides for these intangibles is neither based on the cultural qualification nor it protects against destruction of an object.

Since the findings of the Krupp/I.G. Farben Trials were made under the rules of international humanitarian law applicable in times of occupation, a reference to these trials and the protection of intellectual property would be fitting since, as seen above, the Tallinn Manual 2.0 does provide certain rules on this. However, in Rule 149 'Confiscation and requisition of property' and its Comments, no reference is made to intellectual property or the Krupp/I.G. Farben Trials. On the contrary, the Rule follows the tangibility requirement as found in Additional Protocol I. While Comment 1 refers to the rules of the Hague Regulations, Comment 3 mentions the previous findings that data, as an intangible asset, does not qualify as property, echoing the tangibility requirement from Additional Protocol I and contradicting the findings of the Krupp/I.G. Farben Trials. Subsequently, in Comment 5, which discusses private cyber property, the example provided concerns a privately owned server, a tangible object. Although not present, a reference to intellectual property law and the Krupp/I.G. Farben Trials would be possible and fitting here.

Conclusion

This article set out to explore to what extent intellectual property in cyberspace is protected under international humanitarian law during cyber operations. The legal instruments predating Additional Protocol I used the term 'property', while Additional Protocol introduced the term 'civilian object'. This choice was politically motivated to conciliate different political systems. This introduction initiated a definitional discussion, which appears to be settled by means of references to the tangibility requirement. The term 'civilian object' is broad enough to encompass the immovable and movable property found in the previous legal instruments, provided that they are visible and tangible. The Experts follow this requirement for objects in cyberspace, thereby excluding objects solely existing in a digital form from the definition.

The Military Tribunal ruled in the Krupp/I.G. Farben Trials that intangible property deserves the same protection as 'normal' property. Despite not being explicitly mentioned by the Tribunal, Dinstein and Dinniss argue that this also applies to intangible objects and to intellectual property rights. It should be noted that the Military Tribunal ruled this in a property offences paradigm, i.e. under the rules of booty, seizure, destruction, pillage and plunder.

The term 'civilian object' is broad enough to encompass the immovable and movable property found in the previous legal instruments, provided that they are visible and tangible.

The fact that the the digital object is protected under the property offences paradigm illustrates why the strict tangibility requirement in the targeting paradigm can be considered an inconsistency. The digital object is protected from wanton destruction, but falls outside the scope of civilian objects and is, therefore, outside the scope of protection provided by the principle of distinction and does not have to be taken into account in the principle of proportionality, making it a legitimate target and a potential object of destruction. Evidently, there is a distinct level of protection in both paradigms, stemming from the tangibility requirement introduced by the term 'civilian object', which, in turn, is introduced to circumvent political debate. If the purpose of international humanitarian law is to mitigate civilian suffering by extending protection to property, the exclusion of digital objects is problematic, especially in light of the fact that the term was introduced to forfeit political debate and not to deprive intangibles from their protection, which during the drafting of Additional Protocol I was a common legal concept.

It was found that the introduction of the term 'civilian object' led to a disparity within the two paradigms that are part of one body of rules of international humanitarian law. The protection against property offences is depending on the proprietary relationship: if a product qualifies as property, tangible or intangible, and is privately owned, it falls under the protective scope of the relevant provisions. The protection in the targeting paradigm is depending on the civilian use of the object and the object must be visible and tangible. While this more restrictive protection stems from the introduction of the term 'object' and its definition, it results in a disparity of protection: intangible objects are protected in the property offences paradigm, but are not in the targeting paradigm. This disparity especially manifests itself with regard to cyber-operations taking place in or affecting cyberspace.

A question for further research is if the intangible object can be afforded protection as property under the interpretation of the Krupp/I.G. Faber Trials. It appears *prima facie* that this is possible since the Trials refer to intangible property, especially when considering the protection of digital property under human rights and domestic legal systems. Subsequently, it is important to establish whether this digital property can also be considered a civilian object. Since the tangibility requirement is now limiting the protection of civilians in cyberspace, it is worth exploring if the use of the French word 'biens' offers an interpretation which also includes intangible property, a point also raised by Macak. This would in turn render the omnipresent prefix 'cyber' superfluous and provide civilians with adequate protection, irrespective of the dimension. ■

This article is based on Bunk's thesis which he wrote at the Cyber Operations Department of the Netherlands Defence Academy. The author wants to express his gratitude to the Netherlands Defence Academy, especially Prof. P.A.L. Ducheine and to Leiden University, especially Dr. R.W. Heinsch, for enabling this unique and interesting opportunity. The thesis was awarded runner-up in the 2017 Junior Scholar Award of the International Conference on Cyber Conflict (CyCon) of NATO's Cooperative Cyber Defence Centre of Excellence.

REFERENCES

Anheuser-Busch Inc. v. Portugal [GC]. (2007, January 11). Reports of Judgments and Decisions 2007-I. No. 73049/01.

Bently, L. and Sherman, B. (2008). *Intellectual Property Law*. Oxford, United Kingdom: Oxford University Press.

Biehler, G. (2007). Property Rights for Individuals under IHL. *Archiv des Volkerrechts*. 45(3). 432-441.

Brilmayer, L. (2008). Ownership or Use?. *Harvard International Law Journal*. 49(2). 413-446.

Carrier, M. (2004). Cabining Intellectual Property Through A Property Paradigm. *Duke Law Journal*. 54(1). 1-145.

Dinstein, Y. (2009). *International Law of Belligerent Occupation*. Cambridge, United Kingdom: Cambridge University Press.

Dinstein, Y. (2010). *The Conduct of Hostilities Under the Law of International Armed Conflict*. Cambridge, United Kingdom: Cambridge University Press.

Final Record of the Diplomatic Conference of Geneva of 1949. Volume II section A. Retrevied from https://www.loc.gov/rr/frd/Military_Law/pdf/Dipl-Conf-1949-Final_Vol-2-A.pdf

Geiger, C. (2009). Intellectual Property Shall Be Protected? *European Intellectual Property Review*. 31(2). 113-117.

Hansen, H. C. (2008). *Intellectual Property Law and Policy: Volume 10*. Oxford, United Kingdom: Hart Publishers.

Harrison Dinniss, H. (2014). *Cyber Warfare and the Laws of War* (2014). Cambridge, United Kingdom: Cambridge University Press.

Helfer, L. R. (2009). The New Innovation Frontier? *Harvard International Law Journal*. 49(1). 1-52.

Henckaerts, J. and Doswald-Beck, L. (eds.). (2009). Customary International Humanitarian Law. Volume 1: Rules. Cambridge, United Kingdom: Cambridge University Press.

Macak, K. (2015). Military Objectives 2.0. *Israel Law Review*. 48(1). 55-80.

Liivoja, R. and McCormack, T. (2012). Law in the Virtual Battlespace: The Tallinn Manual and the Jus in Bello. In Gill T. (ed.). *Yearbook of International Humanitarian Law Volume 15*. The Hague, The Netherlands: Asser Press.

Macqueen, H.. Waelde, C. and Laurie, G. (2007). *Contemporary Intellectual Property: Law and Policy*. Oxford, United-Kingdom: Oxford University Press.

Miles, D. (2011, October 27). Cyber Defense Requires Teamwork, Agility. *American Forces Press Service*. Retrieved from: http://archive.defense.gov/news/newsarticle.aspx?id=65846

Pictet, J.S. (1951). The New Geneva Conventions. *American Journal International Law*. 45. 462-475.

Rahmatian, A. (2015). Cyberspace and intellectual property rights. In: Tsagourias, N. T. and Buchan, R. (eds.), *Research Handbook on International Law and Cyberspace* (pp. 72-93). Cheltenham, United Kingdom: Edward Elger.

Sandoz, Y. Swinarski, C. and Zimmerman, B. (1988). Commentary on the Additional Protocols of 8 June 1977 to the Geneva Conventions of 12 August 1949. The Hague, The Netherlands: Martinus Nijhoff.

Schmitt, M.N. (2015). The Notion of 'Objects' during Cyber-Operations: A Riposte in Defence of Interpretive and Applicative Precision. *Israel Law Review*. 48(1). 81-109.

Schmitt, M. N. (2017). Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations. Cambridge, United Kingdom: Cambridge University Press.

Somu, C. S. (2006). Intellectual Property Rights in Cyberspace. *Paradigm*. 10(1). 62-68.

The United States of America vs. Alfried Krupp, et al. (1949). Judgement, Case No. 58. As found in Law Reports Of Trials Of War Criminals. Selected And Prepared By The United Nations War Crimes Commission, Volume X: The I.G. Farben And Krupp Trial.

The United States of America vs. Carl Krauch, et al. (1949). Judgment, Case No. 57. As found in Law Reports Of Trials Of War Criminals. Selected And Prepared By The United Nations War Crimes Commission. Volume X: The I.G. Farben And Krupp Trial.

United States Department of Defense (2011). *Strategy for Operating in Cyber Space*. Retrieved from: https://csrc.nist.gov/presentations/2011/department-of-defense-strategy-for-operating-in-cy

Van der Kooij, P. A. C. E. (2015). *EU IP Law: a short introduction to European intellectual property law*. Amsterdam, The Netherlands: DeLex.

ANALYSIS

JAPAN: EMERGING CYBER POWER IN ASIA-PACIFIC

MARTA PRZYWAŁA

is Research Fellow in the Kosciuszko Institute and CYBERSEC Project Manager. Her main areas of expertise are cybersecurity, as well as international security and defence. She graduated in French language and literature at the Jagiellonian University in Krakow. She holds double MA degree from the Centre for European Studies of the JU and Institut d'études politiques of the University of Strasbourg. She was granted the French government fellowship.

Japan's security policy was rather passive until the end of the 20th century. In the view of significant changes in the Asia-Pacific region, which started to take place after the Cold War and are still ongoing, Japan needs to redefine its security policy, which was not really a priority in the past. If Japanese authorities aspire to take over the role of a regional leader, they must be ready to face new type of threats in the reality wherein the U.S.-Soviet bipolar system has been gone for decades, with China rising as economic and military power, North Korea threatening to push their nuclear button and Russia pursuing its revisionist foreign policy. Over the last years, the Japanese government has laid structural and legal foundations for becoming a serious player in cyberspace. Even though it is not the case yet, Japan is setting out on its path to become a new global 'cyber power'.

Economy over military

Geopolitical imperatives that governed Japan's behaviour in the modern era[1] changed with the World War II victory of the United States which deprived the country of its sovereignty. The occupant restored Japan at the price of a new constitution renouncing the maintenance of land, sea and air forces, and, in this manner, securing American strategic interests and its naval domination on the Pacific among others. However, the Japanese were quickly rehabilitated and even enjoyed the security that the country had attempted to win for itself through conquest, but without having to bear the accompanying fiscal burdens. Both the 1952 San Francisco Peace Treaty and the 1960 Security Alliance with Americans counterbalanced threats from North Korea, Taiwan and the Soviet Union,

[1] These imperatives included above all establishing centralised control and national unity, as well as sovereignty and autonomy in surrounding areas.

even though Japan was encouraged to rebuild some military power – the Japan Self-Defence Forces were formed with the assistance of the United States.

The latter was there to make the Asian nation-state its strong ally, mainly economically. Preferential access to American technology and to the massive consumer market was granted to Japanese manufacturers. The U.S. also tolerated protectionist policies that Japan used to boost its domestic economy, such as capital controls to ensure domestic investment and depreciated currency to promote exports. Under these new circumstances, the country was back on the trail toward achieving its geopolitical goals, but this time, while defining them, it prioritised economic growth over defence spending. It concentrated more on soft power measures: development assistance, direct and indirect foreign investments, and cultural promotion. As a result, Japan experienced 'an economic miracle' in the 70s and 80s, and in the quest to become a great power, it reached the unquestioned regional dominance as the world's second largest economy (Iyoda, 2010 p. 95).

The growing economy and the attendant, increasing need for imported raw materials raised the fear of overdependence on the outside world, as well as of the events getting beyond the control of Tokyo. There was no military option to reduce the vulnerability of the country as the armed forces were limited and destined to protect its home islands. The U.S. security umbrella was spreading out over external sources of danger. But such reliance is always a risk. When the Cold War finished, Washington no longer had much reason to favour Japan. Its preferential policies had done a lot to boost the country's economy which, over time, actually made Japan capable of rivaling the United States' dominance in this matter. The Western ally wanted Japan to be a strong example of capitalism in East Asia to counterbalance communism, but after the Soviet machine collapsed, there was no need for it any more. The diminishing U.S. role as the offshore balancer to potentially revisionist states in the region resulted in Japan's increased responsibility for developing its own defence and security capabilities.

After the Cold War

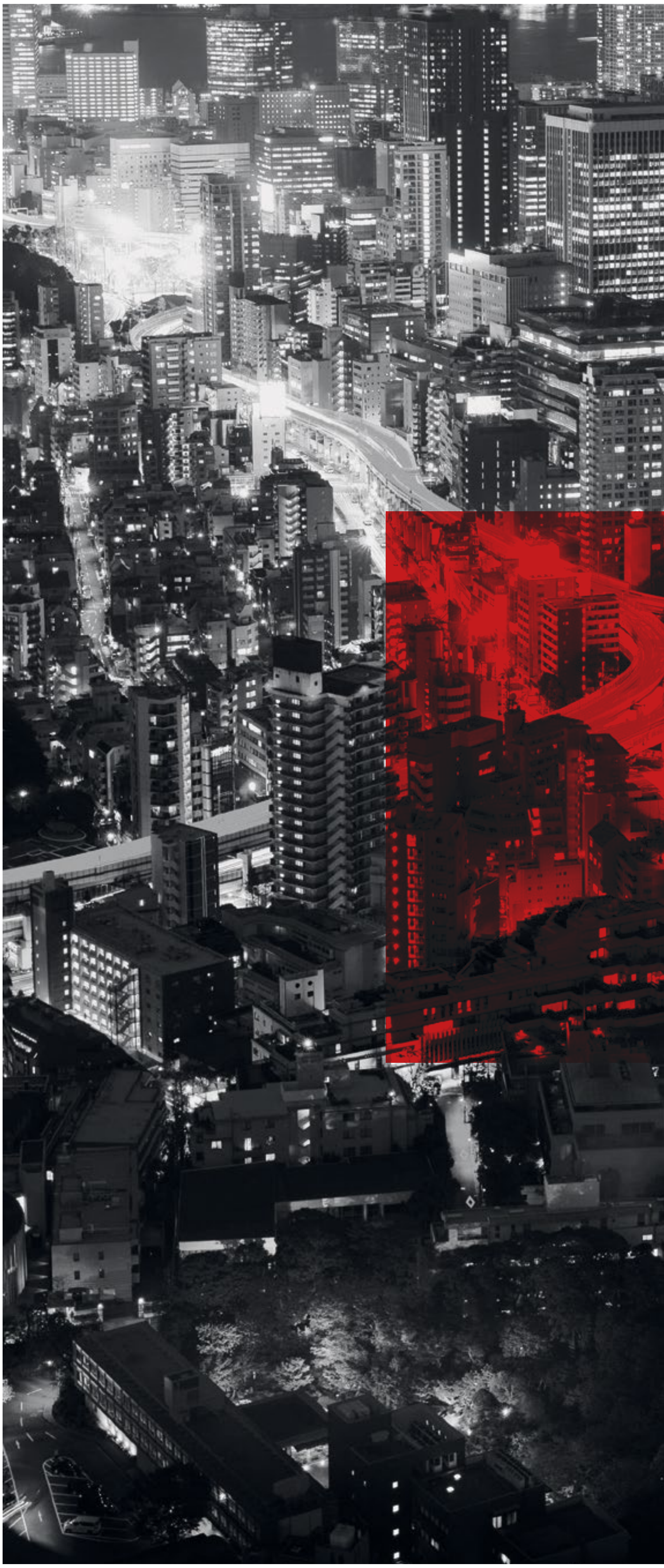
In the new reality, Japan continues to depend on Asia's raw materials and China's growing buying power, which are vital to its prosperity. The difference now is that China is continuing its spectacular rise to power, eroding Japan's longstanding position of a regional hegemon, and the U.S. is no longer afraid of worldwide expansion of communism that previously ensured Japan's security.

'As the liberal theory of international relations predicts, actors with an interest in another country's prosperity are reliable voices for peace. But, as international realists point out, China's growing military shadow is unsettling nonetheless because capabilities can, in theory, influence intentions. If bargaining power comes from the relative costs and benefits of using force, China is clearly gaining an advantage.' (Kohno & Rosenbluth, 2008, p. 6) China is entering a new period in its history. Having accumulated resources from remarkable economic achievements, it is taking a leadership role grounded in this advantageous position. Japan, meanwhile, is pulling out of an extended economic malaise after the collapse of asset markets inflated by years of protectionist regulations. Since 2012, it has been doing invariably well.[2] However, the very source of tensions between China and Japan centers not so much on economy, but on the issue of which country will be the regional leader and will influence big and small geopolitical outcomes. Tokyo might perceive China's quest for hegemony in Asia as alarming because rising powers tend to be 'revisionist' and apt to change the status quo through territorial or economic expansions (vide the Russian Federation). The Japanese feeling of insecurity towards its neighbour is amplified by territorial disputes, historical animosity and China's implacable opposition to a more prominent role of Japan in the United Nations Security Council. Kohno and Rosenbluth (2008) have a neorealist hypothesis that Japan, for its part, is on a quest to gain a 'normal country' status being motivated by a desire to create a balanced, multipolar system in East Asia. Therefore, Japan's military build-up has been and will be a temporal and substantive response

[2] The recent 'Abenomics expansion' noted in the 58-month period from December 2012 to September 2017 now ranks as Japan's second-longest expansion since the end of World War II (Akiyoshi, 2018, January 10).

to China's military expansion. One can also add to that potential and actual threats from North Korea and Russia.

The very source of tensions between China and Japan centers not so much on economy, but on the issue of which country will be the regional leader and will influence big and small geopolitical outcomes.



Back in the game

The rise of China, both economic and military, caused Japan to speed up its military reform, which the United States encouraged. The North Korean regime's frequent sabre-rattling also gave Tokyo a good excuse to undertake rearmament. What is especially interesting is that the country's recent efforts in cyberspace reflect its ambition to have a more proactive military posture and expand the scope of international activity. Given Japan's technological potential, its well established, assessed third in Asia-Pacific in terms of trends and developments, ICT market with global reputation for excellence and innovation (ITU, 2017), the island state can become an important cyber player on a global scale, also due to the steps taken by the current Abe administration to enhance Japan's cyber defence capabilities, as well as the country's position as a central U.S. diplomatic, economic, and military ally in the region. It can be even stated that Japan has initiated a trajectory of a nascent 'cyber power', even though it is not seen as such yet.

To cut a long story short, Japan became serious in its intent regarding cybersecurity, which is reflected in broader trends of change and new assertiveness in its overall security trajectory. Japanese decision-makers take notice of deep connections between cybersecurity and many other dimensions of human activity. With its Cybersecurity Strategy from 2015, Japanese policy-makers moved cybersecurity to the very core of the national security policy. They have been continuously creating more centralized frameworks and means of defensive cybersecurity in the domain (e.g. within Japan's Cyber Clean Center, JPCERT/CC, National Center of Incident Readiness and Strategy for Cybersecurity – NISC, Cybersecurity Strategic Headquarters, and Industrial Cybersecurity Promotion Agency – ICPA).

Japan has also begun to militarize its response by moving the cybersecurity elements of previously purely civilian concern to its principal military institutions, namely the Japan Ministry of Defence (JMOD) and Japan Self-Defence Forces (JSDF), in order to deter cyber threats more effectively.[3] Since 2011, the Japanese have got a substantial section in the JMOD annual white paper *Defence of Japan* and got placed alongside weapons of mass destruction and international terrorism as the most immediate of regional and global security concerns. Japan has begun to militarize its cybersecurity in response to a series of incidents that revealed country's cybersecurity vulnerabilities.

> ***Japan became serious in its intent regarding cybersecurity, which is reflected in broader trends of change and new assertiveness in its overall security trajectory.***

Since 2009, an increased volume of advanced persistent threats (APTs) attacking Japan's critical infrastructure has been noted. Although North Korea and Russia are mentioned, China is most often cited as the prime instigator of the attacks seeking to steal strategic information from competitors and leading industrialized nations (Kallender & Hughes, 2016). Security researchers at Secureworks investigated activities associated with the Bronze Butler threat group, which they assess has been operating out of China since at least 2012 (Secureworks, 2017). The group's operations suggest a long-standing intent to exfiltrate intellectual property and other confidential data from Japanese organisations. Intrusions observed by the researchers indicate a focus on networks involved in critical infrastructure, heavy industry, manufacturing, and international relations. In 2017, the Rand Corporation issued a comprehensive report on China's attempts to shift the status quo in the region without firing a shot through the use of 'gray zone' coercion focused on three domains: maritime, cyber and space (Harold, Nakagawa, Fukuda, Davis, Kono, Cheng & Suzuki, 2017).

[3] However, the JMOD is set to outsource part of its cybersecurity operations to the private sector to bypass training needs for its own staff. The ministry also plans to allow personnel from the private sector to join cybersecurity units in Self-Defence Forces on short-term contracts to promote personnel exchanges. (Defense Ministry..., 2018, May 20)

The Japanese government recognises that cyber groups in China — acting either independently or with China's covert support—seek to attack Japanese websites and conglomerates. As long as their activities do not result in a state of national emergency, they will continue to fall within the realm of petty crime. There has been hardly any Japanese offensive action targeting Chinese websites. Japan's capabilities are more defensive due to the aforementioned Japanese constitution which prohibits war other than for self-defence. However, the current Abe administration is persistently pushing for a revision of the Japanese constitution by 2020 (Rich, 2017, May 3).

Cyber alliances all over the world

In conjunction with the development of a national security strategy, Japan has been actively engaged in diplomatic and trade negotiations related to cybersecurity. Through the mechanism of the US–Japan alliance, which still remains crucial for the country's diplomatic, economic, and military relations, Japan is deliberately and progressively integrating its capabilities and strategy with those of the United States in order to face down the cyber threats from China and other actors. Within this bilateral framework, the two nation-states promote various efforts in the area of policy consultation, cyber incident response and information sharing. However, Japan is actively expanding the perimeter of bi- and multilateral relations in order to enhance its security. It has been pushing for cooperation with ASEAN – mostly through increased investments by Japanese enterprises to ASEAN states (Ujikane, 2016), Israel (Brummer & Oren, 2017, July 28), India – under the 2+2 dialogue that covers foreign policy issues and security (*India, Japan…*, 2018, June 20), and even Russia (Russia, Japan…, 2018, June 23). As for the latter, the Abe administration seems determined to normalise relations with the Kremlin, which can, however, thwart the efforts to improve Sino-Japanese relations.

To ensure a secure and open Internet for all, recognising the importance of human rights and fundamental freedoms, as it is stated in the Joint Elements document from the 3rd Japan-EU Cyber Dialogue (2018), both actors clearly have a common incentive to work within the coalition of like-minded partners, as China and Russia in particular remain at the opposite end of this vision.

Relations with the EU deserve a special attention, because the values and foundations of the Union bode well for cooperation with Japan in cybersecurity. With regards to their vision of cybersecurity (multi-stakeholder, open, free), the EU and Japan are compatible, therefore able to create a trustful and concordant platform to discuss strategic issues important for both parties. The EU can be considered a 'soft power' in cybersecurity as it aims to secure cyberspace primarily through developing mechanisms and cultures of resilience in order to raise preparedness for cyber disruptions and attacks. Furthermore, the Union as a whole is a very important global political and economic influencer that seeks to engage and project externally its model for cybersecurity and Internet governance based on a multi-stakeholder approach and the principles of mutual responsibility and international cooperation. While the Japanese emphasise deterrence and militarization, which implies closer ties with the U.S. in the area of cyber defence, their broader strategic interests and visions for security in cyberspace may actually encourage them to enter into cooperation with like-minded regional organisations, such as the EU and its member states. In order to address common goals (e.g. research and development) and challenges (critical infrastructure protection, cybercrime, cyber espionage, business environment securisation, privacy), to discuss Confidence-Building Measures for cyberspace, and to lead to implementation of shared policy projects, the UN, the ASEAN Regional Forum, the OECD and NATO seem to be natural forums. To ensure a secure and open Internet for all, recognising the importance of human rights and fundamental freedoms, as it is stated in the *Joint Elements* document from the 3rd Japan-EU Cyber Dialogue (2018), both actors clearly have a common incentive to work within the coalition of like-minded partners, as China and Russia in particular remain at the opposite end of this vision. Japan has national interests in strengthening relations with the EU and its particular member states. A bilateral cyber security cooperation agreement with Estonia – a European cybersecurity leader – is an example of such a will (*Japanese prime minister…*, 2018, January 8).

'States with similar capabilities seek to balance one another in an attempt to avoid war, whereas weaker states, again in an attempt to avoid war, either bandwagon with their stronger rivals or pass the buck by relying on the balancing efforts of their stronger allies.' (Kohno & Rosenbluth, p. 241) Surprisingly, Japan is doing both: trying to counterbalance its rival in economic matters where it is as strong as its adversary and relying on its best allies in defence and security, what seems to be a good strategy so far. Given the political and economic relationships the country has established, as well as the values convergent with those of the Western world, Japan's position is already strong enough to become an active contributor to global peace and stability, including peace and stability in cyberspace. This domain should remain even more important for the island nation-state that has no direct borders with its neighbours and remains isolated from the mainland.

Given the political and economic relationships the country has established, as well as the values convergent with those of the Western world, Japan's position is already strong enough to become an active contributor to global peace and stability, including peace and stability in cyberspace.

Japan's evolving role as a 'cyber power' will potentially increase tensions with China. Especially as the country is expanding its defence perimeter in cyberspace while avoiding a direct cyber dialogue with the neighbour. The mutual distrust can be seen in the absence of bilateral talks on cybersecurity between China and Japan, with only a trilateral cybersecurity dialogue taking place between China, Japan, and South Korea (Hurst, 2018, May 12). This approach is not only likely to cause further direct tensions with China, but can also be a path to an open and broader conflict. Due to various contentious issues, the lack of trust, and different perspectives on cybersecurity, Sino-Japanese cooperation in cyberspace or in any other strategic domain will continue to face major challenges. China, being capable of causing enormous political and military earthquakes, will probably not sit and watch the growing Japan quietly. Japanese decision-makers, while taking proactive measures in cyberspace, need to be mindful of the risks of rapid escalation and conflict even beyond cyberspace if they are not to destabilize bilateral ties and a wider Asia-Pacific region security outlook. ■

REFERENCES

Akiyoshi, T. (2018, January 10). The Japanese Economy in 2018: On Track for a Record-Setting Growth Streak. *Nippon.com*. Retrieved from https://www.nippon.com/en/currents/d00375/

Brummer, M., & Oren, E. (2017, July 28). *Israel and Japan's Rising Sun Relations*. Foreign Affairs. Retrieved from https://www.foreignaffairs.com/articles/japan/2017-07-28/israel-and-japans-rising-sun-relations

Christou, G. (2017). The EU's Approach to Cybersecurity. *EU-Japan Security Cooperation: Challenges and Opportunities*. University of Essex. Retrieved from http://repository.essex.ac.uk/19872/1/EU-Japan_9_Cyber_Security_Christou_EU.pdf

Defense Ministry to outsource cybersecurity work to private sector. (2018, May 20). *The Japan Times*. Retrieved from https://www.japantimes.co.jp/news/2018/05/20/national/defense-ministry-outsource-cybersecurity-work-private-sector/

Harold, S. W., Nakagawa, Y., Fukuda, J., Davis, J. A., Kono, K., Cheng, D., & Suzuki, K. (2017). *The U.S.-Japan Alliance and Deterring Gray Zone Coercion in the Maritime, Cyber, and Space Domains*. RAND Corporation.

Hurst, D. (2018, May 12). China-Japan-South Korea Trilateral (Finally) Meets Again. *The Diplomat*. Retrieved from https://thediplomat.com/2018/05/china-japan-south-korea-trilateral-finally-meets-again/

India, Japan hold 2 plus 2 dialogue. (2018, June 20). *Outlook India*. Retrieved from https://www.outlookindia.com/newsscroll/india-japan-hold-2-plus-2-dialogue/1333448

ITU. (2017). *Measuring the Information Society Report 2017*. Retrieved from https://www.itu.int/en/ITU-D/Statistics/Pages/publications/mis2017.aspx

Iyoda, M. (2010). *Postwar Japanese Economy: Lessons of Economic Growth and the Bubble Economy*. New York, NY: Springer.

Japan Cyber Readiness at a Glance. (2016). *Cyber Readiness Index 2.0*. Potomac Institute. Retrieved from http://www.potomacinstitute.org/images/CRI/CRI_Japan_Profile_PIPS.pdf

Japanese prime minister to visit Baltic states. (2018, January 8). *ERR*. Retrieved from https://news.err.ee/652777/japanese-prime-minister-to-visit-baltic-states

"Joint Elements" from the 3rd Japan-EU Cyber Dialogue. (2018, March 5). *Ministry of Foreign Affairs of Japan*. Retrieved from https://www.mofa.go.jp/mofaj/files/000344032.pdf

Kallender, P., & Hughes, Ch. W. (2016). Japan's Emerging Trajectory as a 'Cyber Power': From Securitization to Militarization of Cyberspace. *Journal of Strategic Studies*. 40(1-2). pp. 118-145.

Kohno, M., & Rosenbluth, F. (2008). Japan and the World: Japan's Contemporary Geopolitical Challenges – A Volume in Honor of the Memory and Intellectual Legacy of Asakawa Kan'ichi. *CEAS Occasional Publication Series*. Book 2. Retrieved from https://elischolar.library.yale.edu/cgi/viewcontent.cgi?referer=https://www.google.com/&httpsredir=1&article=1001&context=ceas_publication_series

Rich, M. (2017, May 3). Shinzo Abe Announces Plan to Revise Japan's Pacifist Constitution. *The New York Times*. Retrieved from https://www.nytimes.com/2017/05/03/world/asia/japan-constitution-shinzo-abe-military.html

Russia, Japan sign MOU on cooperation. (2018, June 23). *Xinhuanet*. Retrieved from http://www.xinhuanet.com/english/2018-06/23/c_137275716.htm

The Geopolitics of Japan: An Island Power Adrift. (2009, August 31). *Stratfor Worldview*. Retrieved from https://worldview.stratfor.com/article/geopolitics-japan-island-power-adrift

Ujikane, K. (2016, May 30). Japan Shifts Investment From China to Southeast Asia. *Bloomberg*. Retrieved from https://www.bloomberg.com/news/articles/2018-07-16/happy-prime-day-jeff-amazon-ceo-s-net-worth-tops-150-billion

BRAIN

POLICY FOR
ARTIFICIAL
INTELLIGENCE

1 GLOBAL TOUR
5 STOPOVERS
365 DAYS

AI FOR INDUSTRY 4.0

AI FOR FINANCE

AI FOR COMMERCE

AI FOR AUTOMOTIVE

AI FOR HEALTH

WRAP-UP

3 TRACKS
through the whole journey

GOVERNMENT

- Law & Regulations
- Standards
- International cooperation
- Public–Private partnership
- Public services

BUSINESS

- Markets
- Labor
- Innovation
- Sustainable growth
- Development economics

SOCIETY

- Social impact
- Privacy & Ethics
- Educational system
- Political processes
- Social communication

www.ik.org.pl/en/projects/brain-policy-for-artificial-intelligence

CYBERSEC

EUROPEAN CYBERSECURITY JOURNAL

SUBSCRIPTION OFFER

Subscribe now and stay up to date with the latest trends, recommendations and regulations in the area of cybersecurity. Unique European perspective, objectivity, real passion and comprehensive overview of the topic – thank to these features the European Cybersecurity Journal will provide you with an outstanding reading experience, from cover to cover.

In order to receive the ECJ, please use the online subscription form at www.cybersecforum.eu/en/subscription

NEW PRICES OF THE ECJ SUBSCRIPTION!

Annual subscription (4 issues) - electronic edition - ~~199 EUR~~ **NEW PRICE 50 €**

Annual subscription (4 issues) - hard copy - ~~199 EUR~~ **NEW PRICE 149 €**

Annual subscription (4 issues) - hard copy & electronic edition - ~~249 EUR~~ **NEW PRICE 199 €**

EUROPEAN
CYBERSECURITY JOURNAL
STRATEGIC PERSPECTIVES ON CYBERSECURITY MANAGEMENT AND PUBLIC POLICIES
ANALYSES · POLICY REVIEWS · OPINIONS
CONTENTS
5
9
16
32
36
52
56
INTERVIEW WITH DR PAUL TIMMERS

THE ECJ IS ADRESSED TO:

- CEOs, CIOs, CSOs, CISOs, CTOs, CROs
- IT/Security Vice Presidents, Directors, Managers
- Legal Professionals
- Governance, Audit, Risk, Compliance Managers & Consultants
- Government and Regulatory Affairs Directors & Managers
- National and Local Government Officials
- Law Enforcement & Intelligence Officers
- Millitary & MoD Officials
- International Organisations Representatives

FROM THE FOLLOWING SECTORS:

- ICT
- Power Generation & Distribution
- Transportation
- Critical Infrastructure
- Defence & Security
- Finance & insurance
- Chemical Industries
- Mining & Petroleum
- Public Utilities
- Data Privacy
- Cybersecurity
- Manufacturing & Automotive
- Pharmaceutical

FOLLOW THE NEWS @CYBERSECEU

EUROPEAN CYBERSECURITY JOURNAL

STRATEGIC PERSPECTIVES ON CYBERSECURITY MANAGEMENT AND PUBLIC POLICIES

The European Cybersecurity Journal is a new specialized quarterly publication devoted to cybersecurity. It will be a platform of regular dialogue on the most strategic aspects of 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.

ISSN: 2450-21113

The ECJ is a quarterly journal, published in January, April, July and October.

THE KOSCIUSZKO INSTITUTE

Citations: This journal should be cited as follows:
"European Cybersecurity Journal",
Volume 4 (2018), Issue 2, page reference

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

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

www.ik.org.pl
www.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.