

VOLUME 4 (2018) ■ ISSUE 3

# 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

**Chief Editors:** Barbara Sztokfisz, Marta Przywała  
*Research Fellows of the Kosciuszko Institute  
CYBERSEC Project Managers*

**Honorary Member of the Board:** Dr Joanna Świątkowska  
*CYBERSEC Programme Director and Senior Research Fellow  
of the Kosciuszko Institute, Poland*

**Honorary Member of the Board:** Dr James Lewis  
*Director and Senior Fellow of the Strategic Technologies Program,  
Center for Strategic and International Studies (CSIS), USA*

**Member of the Board:** Alexander Klimburg  
*Nonresident Senior Fellow, Cyber Statecraft Initiative, Atlantic  
Council; Affiliate, Belfer Center of Harvard Kennedy School, USA*

**Member of the Board:** Helena Raud  
*Member of the Board of the European Cybersecurity Initiative,  
Estonia*

**Member of the Board:** Keir Giles  
*Director of the Conflict Studies Research Centre (CSRC), UK*

**Editor Associate:** Izabela Albrycht  
*Chairperson of the Kosciuszko Institute, Poland*

**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.



**Citations:** This journal should be cited as follows:  
“European Cybersecurity Journal”,  
Volume 4 (2018), Issue 3, 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](http://www.ik.org.pl)  
[www.cybersecforum.eu](http://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.

© 2018 The Kosciuszko Institute  
All rights reserved. The publication, in whole or in part, may not be copied, reproduced, nor transmitted in any way without the written permission of the publisher.

# EDITORIAL



**BARBARA SZTOKFISZ**

**MARTA PRZYWAŁA**

Research Fellows of the Kosciuszko Institute

CYBERSEC Project Managers

Chief Editors of the European Cybersecurity Journal

Dear Reader,

We are happy to hand over to you this special issue of the European Cybersecurity Journal that coincides with the European Cybersecurity Forum – CYBERSEC taking place in Krakow for the fourth time.

The leitmotiv of CYBERSEC 2018 is building and searching for trust in cyberspace – an obvious yet still underestimated goal. Emerging disruptive technologies show trust must be part of systems and processes, but this is a different kind of trust that is customarily placed in traditional actors who use these technologies. As digital transformation can only succeed in a safe cyberspace, a pursuit to strengthen mutual trust is needed more than ever. Kofi Annan, ‘a man of peace in a world of war’, who is present in our thoughts these days, once said: ‘More than ever before in human history, we share a common destiny. We can master it only if we face it together.’ The same rule applies to this brand new reality of our civilization – the cyber reality. The information management in a multi-stakeholder environment requires cooperation, compliance and accountability. The international community has an important role in building the culture of trust and the architecture of cybersecurity in various areas: public, military, business, and education. It should ring alarm bells particularly where the norms of state behaviour and confidence-building measures are not developed. The cybersecurity is, first and foremost, a shared responsibility. These questions, among others, will be discussed at CYBERSEC 2018, while the present European Cybersecurity Journal will complement them with expert insights.

What is important is that the international community should make the new cyber reality inclusive. To quote again the great mind of the turn-of-the-century, ‘young people should be at the forefront of global change and innovation. Empowered, they can be key agents for development and peace.’ Therefore, to satisfy this need, CYBERSEC and the European Cybersecurity Journal will introduce you to Young Leaders who, embracing a new perspective, are able to look ahead in an unconventional way. In the next issues, we will present a series of articles by winners of the contest for ambitious and visionary students from the world’s most renowned academic institutions. However, before reading them, meet them on the conference stage!

Enjoy CYBERSEC 2018 and the read!

*Barbara Sztofisz*      *Marta Przywała*



# CONTENTS

**6** | **INTERVIEW WITH ANTONIO MISSIROLI**

**9** | **INTERVIEW WITH JOHN FRANK**

**14** | **CHANGING THE STATUS QUO — INCREASING TRUST  
OF THE CLOUD WITH CONTINUOUS ASSURANCE**  
*Daniele Catteddu*

**23** | **ERROR 404: DRONE NOT FOUND  
SMARTPHONES AS UNMANNED AERIAL VEHICLE GROUND CONTROL STATIONS:  
AN OVERVIEW OF CYBER-RELATED VULNERABILITIES**  
*Ginevra Fontana*

**34** | **QUANTUM TECHNOLOGIES AND STANDARDIZATION**  
*Tomasz Mazur*

**38** | **BETWEEN CYBER AND PHYSICAL WORLDS: SECURE ENDPOINT DEVICES  
AS THE KEY INTERFACE FOR A BLENDED REALITY FUTURE**  
*Giulia Pastorella, Simon Shiu*





44

**INFORMATION SHARING FOR THE MITIGATION OF HOSTILE ACTIVITY IN CYBERSPACE: COMPARING TWO NASCENT MODELS (PART 1)**

Deborah Housen-Couriel

51

**CAN A PUBLIC TENDER BE A THREAT TO IT INFRASTRUCTURES IN PUBLIC INSTITUTIONS?**

Pawel Sawicki

57

**PROTECTING TODAY AGAINST THE THREATS OF TOMORROW**

Lothar Renner

62

**INDUSTRY'S INITIATIVE TO INCREASE RESILIENCE OF CYBERSPACE: THE CYBERSECURITY TECH ACCORD**

# OUTCOMES FROM THE 2018 NATO SUMMIT IN BRUSSELS

INTERVIEW WITH DR ANTONIO MISSIROLI



## DR. ANTONIO MISSIROLI

is the Assistant Secretary General for Emerging Security Challenges. Prior to joining NATO, Dr. Antonio Missiroli was the Director of the European Union Institute for Security Studies (EUISS) in Paris (2012-17). Previously, he was Adviser at the Bureau of European Policy Advisers (BEPA) of the European Commission (2010-2012); Director of Studies at the European Policy Centre in Brussels (2005-2010), and Senior Research Fellow at the W/EU Institute for Security Studies in Paris (1998-2005). He was also Head of European Studies at CeSPI in Rome (1994-97) and a Visiting Fellow at St Antony's College, Oxford (1996-97). As well as being a professional journalist, he has also taught at Bath and Trento as well as Boston University, SAIS/Johns Hopkins, at the College of Europe (Bruges) and Sciences Po (Paris). Dr. Missiroli holds a PhD degree in Contemporary History from the Scuola Normale Superiore (Pisa) and a Master's degree in International Public Policy from SAIS/Johns Hopkins University.

Thank you, Dr Missiroli, for finding time for this interview in which we would like to talk about the recent NATO Summit in Brussels. It drew attention of the public opinion in several aspects, but few payed attention to the cybersecurity issues that were raised. What did NATO accomplish with respect to cyber policy during the summit in July this year?

**Antonio Missiroli:** As cyber threats to the security of the Alliance become more frequent, complex and destructive, strengthening cyber defences is a top priority for NATO. At their Summit in July 2018, Allies took the next steps in enhancing their defences in the cyber domain. Recognising cyber's contribution to NATO's overall deterrence and defence, they agreed on how to integrate sovereign cyber effects, provided voluntarily by Allies, into the Alliance's operations and missions. Allies also agreed to establish a new Cyberspace Operations Centre.

NATO leaders remain determined to employ the full range of capabilities, including cyber, to deter, defend against and counter the full spectrum of cyber threats, including those conducted as part of a hybrid campaign. To this end, Allies also re-committed to the national delivery of the Cyber Defence Pledge, which is central to enhancing cyber resilience and raising the costs of a cyber attack.

---

***The decisions taken by Allies at the recent Brussels Summit continue to reinforce this approach in order to ensure that NATO remains fit for purpose in the digital era.***

---

Finally, Allies re-affirmed their commitment to act in accordance with international law, as well as their support for a norm based, predictable and secure cyberspace, underscoring the need to further develop partnerships, including partnerships with the industry and academia.

Over the years, NATO's approach to cyber defence has evolved in a measured and responsible manner in response to the cyber threat landscape. The decisions taken by Allies at the recent Brussels Summit continue to reinforce this approach in order to ensure that NATO remains fit for purpose in the digital era.



**National developments concerning the Cyber Defence Pledge engagements were assessed for the first time with regard to set criteria. The outcomes are classified; however, could you still present the general trends and the overall performance of the Allies? How has the general attitude to cyber defence changed? Can we consider the first test for NATO cyber commitments passed?**

What has become obvious in the two years since the Cyber Defence Pledge was made is how cyber defence is now firmly on the Alliance's radar. This was one of the goals of the Pledge—to raise awareness about the need to invest in cyber defence in order to strengthen national infrastructures and networks. The Cyber Defence Pledge and annual reporting have allowed us to draw attention to the topic to generate sustained commitment. Judging from the evidence provided, we can see that all Allies have made progress, especially with regard to policies and strategies and establishing or reviewing national organisational structures. For example, some nations are now on their third or fourth national cyber security strategy, and we are witnessing a trend of establishing cyber commands – military organisations able to support operations in cyberspace. These structures will be important as more Allies recognise that, alongside NATO's own agenda to operate in cyberspace, their militaries will need to have the right capabilities to be able to take advantage of the cyberspace domain.

Nonetheless, challenges remain. Allies report that securing funding remains very important. Allies continue to grapple with the issues of the recruitment and retention of cyber defence experts. Training is also a vital and perennial issue that requires sustained attention.

In conclusion, it is important to recall that the Cyber Defence Pledge is deliberately open ended, because the threat landscape changes, so Allies will always need to be doing more. The Cyber Defence Pledge thus has an important role to play in helping to change perceptions on how cyber defence should be addressed in a sustainable fashion.

---

***It is important to recall that the Cyber Defence Pledge is deliberately open ended, because the threat landscape changes, so Allies will always need to be doing more.***

---

**One of the most concrete cyber initiatives associated with this year's summit is the new NATO Cyber Operations Centre, which NATO defence ministers agreed to create last year. The Centre will be a part of the outline design for the adapted NATO Command Structure. What does the creation of this institution mean exactly, and how will it integrate national cyber capabilities into NATO missions? Given that cyber capabilities differ from conventional ones, could you clarify what the integration means in this context? What will be the mechanism to integrate voluntary national cyber contributions into the military planning process?**

NATO is setting up a new Cyberspace Operations Centre, in Mons, Belgium, to provide situational awareness and coordination of NATO operational activity within cyberspace. This is a major new component of the adapted NATO Command Structure. It is part of our work to make sure NATO is as effective in cyberspace as we are on land, in the air and at sea.

More specifically, the Cyberspace Operations Centre forms a dedicated and centralised entity with the NATO Command Structure. It functions as NATO's theatre-component command for cyberspace and the primary coordination point for NATO's cyberspace operational activities, including the provision of operational cyberspace situational awareness to NATO commanders, as well as the integration of cyber defence into planning and operations.

The Cyberspace Operations Centre, in its role as a coordinator, will also help integrate Allies' national cyber effects into our operations and missions. Allies will nonetheless retain full control over those capabilities. It is important to highlight that this does not change NATO's mandate. NATO remains a defensive Alliance, and acts in accordance with international law. The Cyberspace Operations Centre will be an important contribution to NATO's cyber defences and to our overall deterrence and defence. We expect the Centre to become operational next year.

**How can NATO respond to cyber-enabled information operations and how can the Alliance be effective against such threats? What is its operational capacity in cyberspace?**

NATO will defend all Allies against any threat: in cyberspace, as well as on land, in the air or at sea. Cyber attacks are increasingly used as a tool in the arsenal of hybrid warfare, and so improving our cyber defences forms an important part of NATO's work on countering hybrid warfare.

NATO's IT infrastructure and centralised protection covers over 60 different locations, from the political headquarters in Brussels, through military commands, to the sites of NATO missions and operations. A 200-strong cyber team defends NATO's networks around the clock. This team prevents intrusions, detects, analyses and shares information and conducts computer forensics, vulnerability assessments and post-incident analysis. NATO also has cyber defence rapid reaction teams on standby to reinforce the defences of NATO networks or to help Allies cope with a cyber attack.

NATO and Allies exchange information about cyber threats in real-time, including through a dedicated Malware Information Sharing Platform. NATO also invests in training, education and exercises which bolster the skills of national cyber practitioners. Deepening partnerships with other countries, international organisations as well as with industry and academia represent an important element of NATO's approach to cyber defence. For example, our continuous interaction with the industry helps provide rapid notice and mitigation of cyber attacks against NATO and NATO Allies. During the WannaCry incident in May 2017, we quickly reached out to Allies and our industry partners. The information we exchanged was critical for getting the most up-to-date picture of a rapidly evolving and complex situation.

While much progress has been achieved to bolster NATO and Allied cyber defences, there remains more to be done in view of the rapidly evolving cyber threat landscape.

**The Brussels summit was an opportunity to follow up on EU-NATO cooperation. The two organisations signed a new joint declaration that focuses, among others, on cyber security and hybrid threats. What are the new elements that it introduces in comparison to the previous declaration? How can it enhance the cooperation between the EU and NATO?**

The very essence of NATO is anchored in the notion that more can be achieved when working together. The Brussels Summit highlighted the progress in recent years on enhancing cooperation between NATO and the European Union, including in the area of cyber defence. Continued cooperation to address evolving security challenges and to strengthen capabilities was further welcomed.

Over the last years, we have taken steps to intensify our cooperation on cyber defence with the European Union, notably in the areas of information exchange, training, research and exercises. Real-time information exchange between the incident responses teams of NATO and the EU continues to take place through a Technical Arrangement on Cyber Defence, concluded in 2016. This Arrangement facilitates cooperation at the operational and tactical level between cyber defence experts. As far as the exercises are concerned, we were pleased that last year, the cyber defence staff from the EU were for the first time made full participants in NATO's Cyber Coalition exercise, and NATO experts were recently involved for the first time in the Cyber Europe 2018 exercise.

---

***The very essence of NATO is anchored in the notion that more can be achieved when working together.***

---

As cyber policies and approaches continue to evolve on both sides of Brussels, we are continuing to seek opportunities to deepen our engagement with the EU in a spirit of complementarity and non duplication. Moving forward, we will be looking increasingly at how our respective organisations are equipped to manage and respond to potential cyber crises, particularly given that many activities in cyberspace 'fall below the threshold', so that we can share the best practices and improve readiness. ■

*Questions by Marta Przywata*



## INTERVIEW WITH JOHN FRANK



### JOHN FRANK

is Microsoft's Vice President, EU Government Affairs. In this role, John leads Microsoft's government affairs teams in Brussels and European national capitals on EU issues. John was previously Vice President, Deputy General Counsel and Chief of Staff for Microsoft President and Chief Legal Officer Brad Smith based at Microsoft's corporate headquarters in Redmond Washington. In this role, he managed several teams including the Law Enforcement and National Security team, the Industry Affairs group, Corporate, Competition Law and Privacy Compliance teams and the department's technology and business operations team. For his first eight years at Microsoft, John was based at Microsoft's European headquarters in Paris. Initially he was responsible for the legal and regulatory issues involved in the launch of the Microsoft Network (now MSN). From 1996 to 2002, Mr. Frank led Microsoft's Legal and Corporate Affairs group for Europe, Middle East and Africa focusing on issues including privacy, security, consumer protection and antitrust. Mr. Frank began the company's European Government Affairs program, which focused on advocacy on software and online policy issues. Prior to joining Microsoft, John Frank practiced law in San Francisco with Skadden, Arps, Slate, Meagher & Flom. Mr. Frank received his A.B. degree from the Woodrow Wilson School of Public and International Affairs at Princeton University and his J.D. from Columbia Law School.

**How can private companies contribute to the enhancement of stability and security of cyberspace? How can they cooperate with governments?**

**John Frank:** Cyberspace is largely owned and operated by the private sector, and government cyber offenses pose dangerous risks to stability and security. Technology companies are often the first line of defense and response to online assaults by nation-states or other actors. We need multi-stakeholder action to change government behaviour and to improve cyber defense and resilience.

We are determined to reduce nation-state cyber assaults on civilians through multi-stakeholder action. The WannaCry and NotPetya attacks in 2017 were launched by nation states. They were highly destructive and indiscriminately damaged businesses and citizens around the world. Each caused billions of Euros in damages. But no country has called the assaults a violation of international law.

---

***We need multi-stakeholder action to change government behaviour and to improve cyber defense and resilience.***

---

Governments need to adopt binding international norms for responsible behavior in cyberspace. We commend existing efforts such as the UNGGE process and the Global Commission on the Stability of Cyberspace. But we believe the most effective solution will require a new international agreement – a [Digital Geneva Convention](#) – to protect civilians on the internet in peace and in armed conflicts. This would build on existing international law, establishing clear limits for the permissible use of offensive capabilities in cyberspace. We recognize that incremental steps by governments, the private sector and civil society towards a set of digital peace principles can strengthen the effectiveness of norms of behavior and support diplomatic leadership in this area.

Microsoft and other technology companies also have responsibilities to protect and defend our customers. As a company, we are constantly enhancing our [security measures](#) by leveraging advanced analytics and AI – but we are also taking steps as an industry. Earlier this year we joined over 30 other companies in signing

the [Cybersecurity Tech Accord](#) that pledges to protect customers, oppose nation-state attacks on innocent citizens and enterprises, and partner with each other to enhance cybersecurity. And the initiative has been growing since.

No single government or company can solve a problem of this scale. But with concrete commitments from private and public organizations alike, we can reduce the risks, increase resilience and keep citizens safe, both on- and offline.



***We recognize that incremental steps by governments, the private sector and civil society towards a set of digital peace principles can strengthen the effectiveness of norms of behavior and support diplomatic leadership in this area.***

**This year the US Congress passed The Clarifying Lawful Overseas Use of Data Act, the so-called CLOUD Act. Do you think this particular piece of regulation may significantly help overcome obstacles related to evidence access? What do you think about how cooperation with European entities should look in this matter?**

Microsoft has advocated for new international agreements to reform the process by which law enforcement officials gather digital evidence and investigate crimes. We believe that the adoption of the CLOUD Act was an important step forward in this regard.

The CLOUD Act preserves the right of cloud service providers to challenge search warrants when there is a conflict of laws. But even more importantly, it creates a framework that can provide robust privacy protections while enabling law enforcement agencies to access data in each other's countries.

However, this is not the end of the road. Governments need to move forward quickly in putting new international agreements in place. We believe that these agreements should be principle-based. That is why [we recently announced six bedrock principles](#) to drive our advocacy as governments reform their laws and pursue international agreements that regulate cross-border access to data.

---

***Governments need to move forward quickly in putting new international agreements in place. We believe that these agreements should be principle-based.***

---

These principles are:

1. a universal right to notice;
2. prior independent judicial authorization of law enforcement demands for data;
3. a detailed legal process and ability to challenge such demands;
4. mechanisms to resolve conflicts with third-countries;
5. the right for enterprises to receive law enforcement requests directly; and
6. transparency.

Users have the right to be protected by their own nation's laws. The principles we are articulating represent baseline minimum requirements that should govern law enforcement access to data. Their applications may vary, but the underlying foundation of check-and-balances, accountability and transparency should remain the bedrock of any future agreements on this issue of vital international importance.

**During the 4th edition of the European Cybersecurity Forum, we will discuss the concept of Digital Three Seas – in a nutshell, the idea is that we should aim to build stronger digital cooperation among countries that cooperate under the umbrella of the Three Seas initiative. How can companies like Microsoft contribute to that?**

The Three Seas initiative can help improve economic development and integration across borders. We believe digital strategies can create greater North–South economic connections within the Three Seas Group.

National governments have been slower than European enterprises to embrace digital transformation in their core missions. The Three Seas Group can aspire to build on each other's advances deploying advanced digital solutions for providing governmental services to their citizens. Similar digital solutions across the region will make it simpler for businesses to expand from their home country within the Three Seas Group.

---

***The Three Seas initiative can help improve economic development and integration across borders. We believe digital strategies can create greater North–South economic connections within the Three Seas Group.***

---

Digital transformation is reshaping the competitive dynamics for companies in every country. We are committed to helping ensure that every country within the Three Seas Initiative can reap the benefits of digitization. We work across the region assisting public and private organizations in implementing cloud solutions that improve productivity and efficiency, as well supporting start-ups and equipping young people with the digital skills they need to succeed in the workplace of the future.

We strongly welcome the call for the Three Seas Initiative to expand its digital remit. We believe that regional governments, local digital businesses and global players such as Microsoft can address both needs, opportunities and challenges in the region when working all together. And cybersecurity deserves special focus. Exchanging best practices on cybersecurity to strengthen the region's cyber resilience, pioneering joint research on artificial intelligence, or fostering digital transformation for the region's businesses – these are all key to ensuring the Three Seas members can thrive and grow on the world stage. ■

*Questions by Dr Joanna Świątkowska*







**LEADERS' FORESIGHT**  
FEBRUARY 2019

WASHINGTON ●



# ADVANCING CYBERSECURITY AROUND THE WORLD



**CYBERSEC**

EUROPEAN  
CYBERSECURITY FORUM

ANALYSIS

## CHANGING THE STATUS QUO — INCREASING TRUST OF THE CLOUD WITH CONTINUOUS ASSURANCE



**DANIELE CATTEDDU, CHIEF TECHNOLOGY OFFICER,  
CLOUD SECURITY ALLIANCE**

Daniele Catteddu is an information security and risk management practitioner, technologies expert and privacy evangelist with over 15 of experience. He worked in several senior roles both in the private and public sector.

Currently, he is the Chief Technology Officer, at Cloud Security Alliance, where he is responsible to drive the adoption of the organization technology strategy. He identifies technology trends, global policies and evolving social behavior and their impact on information security and on CSA's activities. Mr Catteddu is the co-founder and director of the CSA Open Certification Framework / STAR Program.

### Introduction: The long tail of cloud computing

Cloud computing is the present and the future of IT; in the space of less than 10 years it has gained a tremendous level of penetration. Today, the vast majority of organisations (Columbus, 2018) like Google and individuals with Internet access use cloud computing in some shape or form. Several renowned analysts concur that this growth trend will only continue (Columbus, 2017).

In today's world, essentially every business sector makes use of cloud services. Governments are making their 'cloud first' (GOV.UK, 2017; Kundra, 2011; NEA, 2017; MDEC, 2018) policy a strategic priority for the modernisation of the public administration, improvement of eGov services, and the leverage of 'open data'. The financial sector institutions are adopting the cloud to gain competitiveness

via reducing their IT cost and gaining agility by empowering their developers to create new added value services. In the research field, large institutions<sup>1</sup> like CERN, ESA, EMBL and many others fully rely on large scale supercomputers to complete analyses and experiments that are changing the history of biology, astrophysics, quantum physics, and mechanics. The list could go on and on, encompassing any aspect of our lives from healthcare to entertainment.

---

***In today's world, essentially every business sector makes use of cloud services. Governments are making their 'cloud first' policy a strategic priority for the modernisation of the public administration, improvement of eGov services, and the leverage of 'open data'.***

---

<sup>1</sup> Europe's Leading Public-Private Partnership for Cloud, <http://www.helix-nebula.eu>

As it often happens when dealing with technology, and in consideration of the pervasiveness of the cloud, cybersecurity has a critical role to play.

This paper will discuss some of the key aspects related to security, privacy, governance and compliance and will propose a new approach and ideas for the cloud security and privacy.

### Cloud security and privacy

In 2009, the European Cyber Security Agency, ENISA, published a paper entitled 'Cloud Computing Risk Assessment: Benefits, risks and recommendations for information security' (2009), a study in which a group of experts investigated the risks and opportunities of cloud computing from the cybersecurity stand point. The results of the analysis were clear; despite some obvious concerns related to the loss of direct control and governance, cloud computing could bring along a higher level of security compared to an on-premise IT infrastructure.

Unfortunately, due to the lack of education and awareness about the cloud model and its underlying technologies, security and privacy have been perceived as the number one barrier to a large scale adoption of the cloud, especially in Europe and Asia. Some technologists and policy makers depicted the cloud as a bubble that was bound to explode under the pressure of ungovernability, a lack of standardisation and transparency, and the complexity of the global legal and regulatory framework. They were wrong in absolute terms since the cloud is still here and will be with us at least up until quantum computers will force the next IT revolution. That said, most of the risks they perceived were real, and it is the duty of all cloud stakeholders to help address them.

---

***Unfortunately, due to the lack of education and awareness about the cloud model and its underlying technologies, security and privacy have been perceived as the number one barrier to a large scale adoption of the cloud.***

---

For instance, it is undeniable that the cloud has brought a loss of direct control over the ICT infrastructure. Unless you are a cloud infrastructure provider (i.e. IaaS), you will not have direct access to server, storage and network components; instead, you will rely on someone else doing the job for you. The most immediate consequence of that is that there is a deterioration of the level of visibility over the network and security events and that a cloud user needs to rely on a trusted relationship with his/her cloud service provider (CSP) in order to compensate such loss of data. This of course implies that the CSP has to provide the customer with enough information to govern his/her business and demonstrate responsibility and accountability toward their customers, business partners and regulators. Such a new approach to governance based on indirect control over the infrastructure demands new strategies and tactics to acquire the information needed to manage the relationships with CSPs; it demands an increased focus on contract terms, SLAs, service documentation and, of course, audits and third party certifications.

It is also undeniable that both CSPs and cloud users are heavily impacted by the fragmentation and complexity of the global legal framework. While the cloud is a global scale phenomenon that relies on the possibility to apply the same practices across the board, the national governments have to look after the national interests and these two perspectives are not necessarily aligned. For many years we have witnessed the campaigns of some European policy makers against USA-based CSPs as a consequence of the (in)famous Patriot Act (2001)<sup>2</sup> and FISA (1978)<sup>3</sup>, and requests to keep data on the European soil. During the pre-GDPR era, we have discussed the diversity, if not the incompatibility of the different Data Protection laws, both within the European Union and at a global level. In general, it is clear that CSPs are under incredible pressure to comply with several international and national requirements as well as sector-specific regulations. Such a proliferation of requirements increases the cost of compliance and potentially creates room for security vulnerabilities. An anecdotal fact might help to further clarify the magnitude of the issue; the major

---

<sup>2</sup> [https://en.wikipedia.org/wiki/Patriot\\_Act](https://en.wikipedia.org/wiki/Patriot_Act)

<sup>3</sup> [https://en.wikipedia.org/wiki/Foreign\\_Intelligence\\_Surveillance\\_Act](https://en.wikipedia.org/wiki/Foreign_Intelligence_Surveillance_Act)



cloud infrastructure providers are currently complying with over 30 (!) sets of different security and privacy frameworks, including international standards, national and sectorial laws, and regulations (*AWS Compliance Programs*, n.d.; *Compliance Offerings*, n.d.; *Standards, Regulations & Certifications*, n.d.). Someone might argue that this is not exactly the most cost-efficient and effective way to show your customers that you care about security and privacy.

---

***The major cloud infrastructure providers are currently complying with over thirty 30 (!) sets of different security and privacy frameworks, including international standards, national and sectorial laws, and regulations.***

---

The loss of control and complexity of the legal and regulatory framework are examples of how the cloud is driving changes within a company's approach to security and privacy.

In general, there are some key factors that any cloud user and CSP should take into consideration to build an effective and efficient security and privacy management system/program:

- **Shared responsibility:** this is one of the key concepts of cloud operations and security; the cloud defines a complex supply chain, and depending on where you stand in such a chain, there is a set of security and operational responsibilities associated with it. Pretending the cloud security is 'someone else's problem' (Somebody else's..., n.d.) will never be the right answer. The answer is typically in the contract where the parties define who is responsible for what. If a certain security responsibility is not defined in the contract, then the user has to figure out how to fill that security gap.
- **Lack of visibility:** the cloud is often described as 'someone else's computer', a direct consequence is that all the security and network logs and events that a user used to collect from his/her own infrastructure, network, and security appliances are not available anymore. What is available now is a much less granular set of security alerts that 'someone else' has pre-analysed for the customer. That is not necessarily a net loss of security, but the user's security operation
- **Inherited security:** the cloud is described in the most simplistic way through its different service models; there are a number of applications accessible via the Internet (SaaS) that use developed platforms (PaaS) and built on top of infrastructure (IaaS), with all the three layers communicating via API. In simple terms, if you are a SaaS provider, you will inherit the (in)security provided by the platform and the infrastructure you are sitting on.
- **Lack of right to audit:** with the cloud being a shared environment, it is virtually impossible to guarantee the right to audit to a customer without facing the risk of jeopardising another customer's security and privacy. For similar reasons the cloud also imposes substantial limitations on users in terms of security assessment and penetration testing. This is the reason why cloud customers and regulators have to mostly rely on third party audits, certification and attestations, such as ISO27001 (*ISO/IEC 27000 family...*, n.d.), SOC2 (SOC 2<sup>®</sup>..., n.d.) , CSA STAR Program (*STAR Certification* n.d.; *STAR Attestation*, n.d.; *STARSelf-Assessment*, n.d.).
- **Reliance on SLA:** good cloud governance relies on good quality metrics and indicators. Service Level Objectives (SLOs) and Service Qualitative Objectives (SQOs) are the most reliable sources of information for a customer as they express CSPs commitments. It is of paramount importance that customers push for the adoption of standard representation of SLOs and SQOs (see *ISO/IEC 19086-1:2016*, n.d.; *ISO/IEC FDIS 19086-2*, n.d.; *ISO/IEC 19086-3:2017*, n.d.) so as to be able to effectively compare different services and properly measure their performance, especially from the security stand point.
- **Evidence-based trust:** as mentioned earlier, third-party certification and attestation are the key pieces of a cloud assurance program, except that they should be considered a condition necessary but not always sufficient to guarantee an adequate level of assurance. Depending on a user's risk appetite and compliance requirements, third-party certification would need

centre (SOC) and incident response team would need to adapt.



to be supported by additional evidence or additional independent measurement of security parameters. In certain business sectors like finance, a customer would need to receive a sufficient amount of data to be able to properly measure and manage the risk it is exposed to.

---

***Third-party certification and attestation are the key pieces of a cloud assurance program, except that they should be considered a condition necessary but not always sufficient to guarantee an adequate level of assurance.***

---

- **Accountability:** to put it in the simplest terms possible, the cloud allows you to transfer security and privacy responsibilities, but not accountability. Each actor in the cloud supply chain is always accountable for his/her duties, which means that even if someone else is doing the job for you, you have to implement an adequate level of due diligence and monitoring.
- **Standardisation:** most of the organisations today rely on several different CSPs, sometimes integrated with an existing on-premise solution. A typical scenario is one or two IaaS providers, a couple of PaaS, and hundreds (if not thousands) of SaaS services. It goes without saying that in such a situation an adequate level of standardisation is required to effectively manage the IT needs of the organisations. Standardisation affects all aspect of technology, from authentication and communication protocols to encryption, to information security controls frameworks and SLAs. Standardisation influences the way a company manages its business, the way it cooperates and works with its providers and partners, approaches security and its procurement practices. Given the strong emphasis that the cloud puts on due diligence and accountability, it is especially important to standardise the process of assessment and evaluation of CSP to be able to compare and benchmark.



## What is missing?

Everything described above is a simplified description of the status quo, a reference to existing good practices. However, in order to make a real breakthrough and fundamentally increase the level of assurance, transparency, and ultimately trust, of the cloud, there is something that we are still missing: continuous assurance.

---

***In order to make a real breakthrough and fundamentally increase the level of assurance, transparency, and ultimately trust, of the cloud, there is something that we are still missing: continuous assurance.***

---

The concept of continuous assurance is directly connected to the ideas of continuous auditing (see for instance Groomer and Murthy, 1989; and Vasarhelyi and Halper 1991) and continuous monitoring. The two concepts have been around for the last 30 years, but have found some practical barriers for their full scale implementation. As it is outside the scope of this short paper to discuss in depth the evolution of the concept of continuous auditing, monitoring and assurance, it will limit itself to quoting the definition of continuous auditing created by the Cloud Security Alliance in the context of the project EU-SEC<sup>4</sup>:

**‘Continuous Auditing** is an on-going audit process that aims to assess Service Qualitative Objectives (SQOs) and Service Level Objectives (SLOs) conducted at a frequency requested by the purpose of audit (EUSEC, 2017)’. The idea is, in fact, to conduct an ongoing audit process in order to overcome the limitations of any ‘point in time’ assessment and, consequently, provide a more precise insight into the security and the privacy posture of an organisation.

In reality, some CSPs have already implemented continuous monitoring and auditing and built programs for continuous assurance. But all of them have a fundamental limitation, i.e. they are proprietary, not standardised, programs that provide a good picture of a specific CSP’s posture, but do not offer the user a unique view of all the CSP in its

vendor portfolio. This means that the burden of normalising the input from the various CSP is on the user’s shoulders. Besides being a cost and a limit to industry benchmarking, this standardisation effort can potentially suffer from a knowledge gap on the part of the user, since the normalisation exercise is certainly not trivial.

For some time now, the Cloud Security Alliance (CSA) has been one of the organisations that have put a lot of effort in the identification of a solution for continuous assurance, particularly for the creation of a continuous auditing-based certification. Such an effort is being made under the CSA STAR Program.

## The CSA STAR Program

Initiated in 2011, CSA STAR is a program for cloud provider assurance. The STAR program provides the industry with multiple tools:

- The STAR Registry is a publicly accessible website where cloud providers post both self-assessments and third-party audits based upon CSA cloud security standards. By insisting upon cloud provider transparency, CSA is delivering a level of detail around security practices previously only available under non-disclosure agreement (NDA). CSA STAR has been adopted by all of the major cloud providers and hundreds of others (CSA *Security, Trust & Assurance Registry*, n.d.). The STAR program is structured around three levels of assurance: 1) STAR Self-Assessment, 2) STAR Certification/Attestation, and 3) STAR Continuous.
- Cloud Controls Matrix (CCM) as a controls framework, the CSA CCM provides both cloud providers and customers with the needed structure, detail and clarity relating to information security tailored to cloud computing. The CCM provides the fundamental cloud control objectives with context around provider versus customer control responsibilities, as well as the mappings to other popular standards, such as PCI/DSS, ISO/IEC 27001, COBIT, NIST 800-53 and many more.
- The Consensus Assessments Initiative Questionnaire (CAIQ) (*Consensus Assessments...*, n.d.) – drawing upon the CCM, the CAIQ provides a set of Yes/No/NA

---

<sup>4</sup> The European Security Certification Framework (EU-SEC), <https://www.sec-cert.eu>

questions a cloud consumer and a cloud auditor may wish to ask a cloud provider to ascertain their compliance to the Cloud Controls Matrix and CSA best practices.

Typically, enterprises adopt the CSA STAR program in the following ways:

1. Cloud Controls Matrix is used by enterprises as a controls framework baseline for their transition to cloud computing. It is usually mapped against the internal ISMS.
2. Enterprises query the STAR Registry to search for cloud providers they are interested in procuring or otherwise evaluating. The provider STAR entries provide valuable information that can be compared to the customer requirements.
3. If the cloud provider does not appear in the STAR Registry, customers typically send the provider the Consensus Assessments Initiative Questionnaire (CAIQ). Virtually all providers have experience with the CAIQ and will provide a completed copy relatively quickly, although in some cases an NDA is necessary.

Currently, CSA is working on an additional component of the STAR Program called STAR Continuous which is expected to be released before the end of 2018.

### What is CSA STAR Continuous?

STAR Continuous is a module in the CSA STAR Program that gives CSPs the opportunity to integrate their approach to cloud security compliance and certification with additional capabilities to validate their security posture on an ongoing basis. It specifies necessary processes that will be executed during the validation of controls in the scope of the assessment. It also provides a governance structure to facilitate the establishment of trust over its implementation. STAR Continuous does this by specifying the necessary activities and conditions for the implementation of an approach that will lead to continuous auditing-based certification, like for instance the operationalisation of security and privacy requirements.

The STAR Continuous is built to provide a higher assurance and confidence, as it integrates current approaches to assessment with a more frequent verification over the implementation of security controls.

### The STAR Continuous gives the opportunity to:

- Ensure that proper security controls are in place at any given point in time
- Support automated verification that the controls are being met
- Provide transparent visibility into the controls
- Make frequent updates to the STAR Self-Assessment: STAR Continuous Self-Assessment.
- Support third-party based certification (e.g. STAR Certification) with additional and updated information on the CSP security posture: STAR Certification/ Attestation + STAR Continuous Self-Assessment
- Establish a process to continuously audit a CSP security program or ISMS and offers proof of an ISMS that goes beyond just the basic compliance certification model and for proof that there is a process in place that continually monitors critical aspects of the system: STAR Continuous Auditing.

### In addition, STAR Continuous can help CSPs to:

- Provide top management with greater visibility so that they can evaluate the effectiveness of their management system in real-time in relation to expectations of the internal, regulatory and cloud security industry standards
- Implement an audit that is designed to reflect how your organisation's objectives optimise cloud services
- Demonstrate progress and performance levels that go beyond the traditional 'point in time' scenario.

### For customers of cloud service providers


#### STAR Continuous:

- Will provide a greater understanding of the level of controls that are in place and their effectiveness.

### What is the user case for STAR Continuous?

If you are a CSP holding sensitive corporate data that must be compliant with the GDPR or provides business critical applications, having a comprehensive story around how the data and systems are protected and having that story continuously validated will reduce the apprehension customers have before they move their business to you. More and more organisations are evaluating cloud options first before making any new IT investments. While organisations embrace the cloud to reduce the complexity and costs of traditional IT, there is still apprehension from some CIOs to transfer services into the cloud.

Security controls, compliance, and the call for increased transparency are rapidly becoming the baseline expectations of users – especially enterprise customers. Increasing reliability of results, transparency, and ease of use of the CSP's assurance reports is a competitive advantage in today's environment and it might become an entry barrier for those who have not made the investment in a continuous auditing-based accreditation.



***Security controls, compliance, and the call for increased transparency are rapidly becoming the baseline expectations of users – especially enterprise customers.***

STAR Continuous improves on the traditional point-in-time certification. While a point-in-time certification chiefly relies on trust right after a manual audit is conducted, continuous auditing allows increasing the frequency of the auditing process and, therefore, making precise statements on the compliance status at any time over the whole timespan in which the continuous audit process is executed, achieving an 'always up-to-date' compliance status.

Essentially, the proposed framework starts from a simple certification of the timely submission of self-assessment compliance reports and moves up to continuous certification of the fulfilment of control objectives.

### Help change the Status Quo

The Cloud Security Alliance (CSA) is a not-for-profit organisation dedicated to the development of best practices for cloud security and privacy. Its mission is to increase the level of assurance, transparency and trust within the cloud market and beyond. The vast majority of the work the CSA does is developed thanks to the support of volunteers and most of the intellectual property it generates is freely available to anyone.

Please consider contributing to the refinement of the work the CSA has already done in the context of the STAR Program, specifically in the area of continuous auditing. The standardisation of such a sophisticated process is not a trivial task and requires expertise and consensus.

You can learn more about the STAR Program and ways to contribute on the CSA's website at: [cloudsecurityalliance.org/star](https://cloudsecurityalliance.org/star) ■

## REFERENCES

---

*AWS Compliance Programs.* (n.d.) Amazon. Retrieved from: <https://aws.amazon.com/compliance/programs/>

*Cloud Controls Matrix Working Group.* (n.d.). CSA. Retrieved from: [https://cloudsecurityalliance.org/group/cloud-controls-matrix/#\\_overview](https://cloudsecurityalliance.org/group/cloud-controls-matrix/#_overview)



- Columbus, L. (2018, January 7). 83% Of Enterprise Workloads Will Be In The Cloud By 2020. *Forbes*. Retrieved from: <https://www.forbes.com/sites/louiscolombus/2018/01/07/83-of-enterprise-workloads-will-be-in-the-cloud-by-2020/#1a62a3696261>
- Columbus, L. (2017, April 29). Roundup Of Cloud Computing Forecasts, 2017. *Forbes*. Retrieved from: <https://www.forbes.com/consent/?toURL=https://www.forbes.com/sites/louiscolombus/2017/04/29/roundup-of-cloud-computing-forecasts-2017/#f7ee5ec31e87>
- Compliance Offerings. (n.d.). Microsoft. Retrieved from: <https://www.microsoft.com/en-us/trustcenter/compliance/complianceofferings>
- Consensus Assessments Working Group. (n.d.). CSA. Retrieved from: [https://cloudsecurityalliance.org/group/consensus-assessments/#\\_overview](https://cloudsecurityalliance.org/group/consensus-assessments/#_overview)
- CSA Security, Trust & Assurance Registry. (n.d.). CSA. Retrieved from: [https://cloudsecurityalliance.org/star/#\\_registry](https://cloudsecurityalliance.org/star/#_registry)
- ENISA. (2009). *Cloud Computing Risk Assessment: Benefits, risks and recommendations for information security*. Retrieved from: <https://www.enisa.europa.eu/publications/cloud-computing-risk-assessment>
- EUSEC. (2017.) D1.4 Principles, Criteria And Requirements For A Multi-Party Recognition And Continuous Auditing Based Certifications. p. 38. Retrieved from: <https://cdn0.scrvt.com/fokus/15cde3d2c6267d70/82ed8f0cc69c/D1.4-multiparty-recognition-V-1.0.pdf>
- Foreign Intelligence Surveillance Act. (n.d.). Wikipedia. Retrieved from [https://en.wikipedia.org/wiki/Foreign\\_Intelligence\\_Surveillance\\_Act](https://en.wikipedia.org/wiki/Foreign_Intelligence_Surveillance_Act)
- GOV.UK. (2017). *Government Cloud First policy*. Retrieved from: <https://www.gov.uk/guidance/government-cloud-first-policy>
- Groomer, S. M., and Murthy, U. S. (1989). Continuous auditing of database applications: An embedded audit module approach. *Journal of Information Systems*. 3(2).
- ISO/IEC 19086-1:2016. (n.d.). ISO. Retrieved from: <https://www.iso.org/standard/67545.html>
- ISO/IEC FDIS 19086-2. (n.d.). ISO. Retrieved from: <https://www.iso.org/standard/67546.html>
- ISO/IEC 19086-3:2017. (n.d.). ISO. Retrieved from: <https://www.iso.org/standard/67547.html>
- ISO/IEC 27000 family - Information security management systems. (n.d.). ISO. Retrieved from: <https://www.iso.org/isoiec-27001-information-security.html>
- Kundra, V. (2011). *Federal Cloud Computing Strategy*. U.S. Department of the Interior. Retrieved from: <https://www.dhs.gov/sites/default/files/publications/digital-strategy/federal-cloud-computing-strategy.pdf>
- MDEC. (2018). *Making "Cloud First" A Reality For Malaysia*. Retrieved from: <https://mdec.my/blog/?p=165>
- NEA. (2017). *Cloud First Policy*. Retrieved from: [http://www.nea.gov.bh/Attachments/iGA\\_Cloud-First\\_Policy\\_V1.0.pdf](http://www.nea.gov.bh/Attachments/iGA_Cloud-First_Policy_V1.0.pdf)
- Patriot Act. (n.d.). Wikipedia. Retrieved from [https://en.wikipedia.org/wiki/Patriot\\_Act](https://en.wikipedia.org/wiki/Patriot_Act)
- SOC 2® - SOC for Service Organizations: Trust Services Criteria. (n.d.). AICPA. Retrieved from: <https://www.aicpa.org/interestareas/frc/assuranceadvisoryservices/aicpasoc2report.html>
- Somebody else's problem. (n.d.). Wikipedia. Retrieved from [https://en.wikipedia.org/wiki/Somebody\\_else's\\_problem](https://en.wikipedia.org/wiki/Somebody_else's_problem)
- Standards, Regulations & Certifications. (n.d.). Google Cloud. Retrieved from: <https://cloud.google.com/security/compliance/>
- STAR Attestation. (n.d.). CSA. Retrieved from: [https://cloudsecurityalliance.org/star/attestation/#\\_overview](https://cloudsecurityalliance.org/star/attestation/#_overview)
- STAR Certification. (n.d.). CSA. Retrieved from: [https://cloudsecurityalliance.org/star/certification/#\\_overview](https://cloudsecurityalliance.org/star/certification/#_overview)
- STAR Self-Assessment. (n.d.). CSA. Retrieved from: [https://cloudsecurityalliance.org/star/self-assessment/#\\_overview](https://cloudsecurityalliance.org/star/self-assessment/#_overview)
- Vasarhelyi, M. A. and Halper, F. B. (1991). The continuous audit of online systems. *Auditing: A Journal of Practice and Theory*. Retrieved from: <http://citeseerx.ist.psu.edu/viewdoc/summary?doi=10.1.1.364.7964>



# CYBERSEC

YOUNG LEADERS

This year, the European Cybersecurity Forum – CYBERSEC introduces a new initiative addressed to young, ambitious and visionary students interested in strategic and interdisciplinary aspects of cybersecurity.

The Call for Papers announced a few months ago among the most renowned academic institutions of the entire world resulted in dozens of applications. Authors of best papers were selected and invited to the specially dedicated panel discussion entitled Young Cybersecurity Leaders Looking Ahead!



ANALYSIS

# ERROR 404: DRONE NOT FOUND SMARTPHONES AS UNMANNED AERIAL VEHICLE GROUND CONTROL STATIONS: AN OVERVIEW OF CYBER-RELATED VULNERABILITIES



GINEVRA FONTANA

Master's Student in International Security Studies at Scuola Superiore Sant'Anna & University of Trento. Selected Student at Collegio Clesio. Collaborator at the Center for Cyber Security and International Relations Studies of the University of Florence. Particularly interested in Armed Conflicts, Cybersecurity, Arms Trade and Terrorism Studies.

## 1. Introduction

The US Army began utilising Unmanned Aerial Vehicles (UAVs) in the 1980s. At the time of writing, it owns an extensive array of more than 7,000 of such devices – and seems set on acquiring many more in the future.

Reports from 2016 suggest that the US Army considered purchasing commercial off-the-shelf UAVs for intelligence, surveillance and reconnaissance (ISR) purposes. As such devices are usually controlled with a smartphone or a tablet, this article tries to answer the question of what cybersecurity threats such controllers bring into the picture, and how some of these vulnerabilities could be solved.

## 2. Framing the current situation

Unmanned Aerial Vehicles, commonly referred to as *drones*, are a specific type of technological device that, as the name suggests, is a flying robot that is either controlled by a human operator at a distance or is completely independent (Pullen, 2015). The latter typology is still undergoing implementation, but the former has been increasingly tested and used by military agents throughout the past decade. The technology grew more and more accessible, giving way in the past five years to a spill-over effect into the civilian market (Hsu, 2017). Especially when it comes to UAVs used for filmography and videography purposes, the costs became more and more approachable, therefore bringing an increase in their usage (Glaser, 2017).

The US army has used UAVs for ISR since the 1980s (Springer, 2013). At present, the US operate various types of UAVs in war zones: they have a fleet of more than 7,000 remotely piloted aircraft (RPA). A few hundred of these are the infamous MQ-1 Predator and its descendant, the MQ-9 Reaper (Walker, 2017). Used for both ISR and strikes in areas such as Iraq, Pakistan and Afghanistan, these UAVs have come under fire in the public opinion for the discrepancy between the official narrative and the actual outcome of their strikes. In fact, according to various sources, including official ones, Predator and Reaper strikes are not as effective and 'surgical' as they have been portrayed, causing numerous civilian deaths (Chamayou, 2014; Stanley, Fontana & Duraccio, 2017).

---

**The US army has used UAVs for ISR since the 1980s. At present, the US operate various types of UAVs in war zones: they have a fleet of more than 7,000 remotely piloted aircraft. A few hundred of these are the infamous MQ-1 Predator and its descendant, the MQ-9 Reaper.**

---

Although Predators and Reapers are the most talked about, the majority of the US UAV fleet consists of drones primarily used for ISR purposes. Among these, the most numerous are the RQ-11 Ravens, which are more than 7,000 units (Thompson, 2011; Air Force Technology, n.d.). Nonetheless, there has recently been a new addition to the catalogue.

In May 2016, an article published in the online magazine Popular Mechanics mentioned how the US armed forces were looking for new small UAVs (Hambling 2016). Particularly important were a few key elements:

The specifications also demands [sic] a drone that can be readied and launched in less than 60 seconds, from the prone position or under cover. This is in contrast to the Raven, which takes a few minutes to assemble and needs to be thrown into the wind – not so easy when you are under fire. (Hambling 2016)

Moreover, these UAVs needed to be easily operable in enclosed spaces, such as buildings, for ISR—an ability that the ones concurrently owned by the US armed forces did not have (Hambling, 2016).

In January 2017, Wired magazine first reported that the US Marine Corps were considering buying off-the-shelf UAVs to be used in the military field, especially for future 'urban reconnaissance'. More specifically, the article indicated Commandant Robert Neller's will to provide 'every deployed Marine infantry squad to have their own [UAV] for aerial reconnaissance by the end of 2017' (Hsu, 2017).

Off-the-shelf UAVs are usually operated via smartphone or tablet. I have, therefore, decided to analyse the issues that using such technologies to operate UAVs would bring into the mission from the cybersecurity perspective.

### Unmanned Aerial Vehicles: the basics

Understanding the susceptibilities of UAV systems requires a general explanation of how these systems work. Figure 1 shows a simplified model of the basic elements of a UAV.

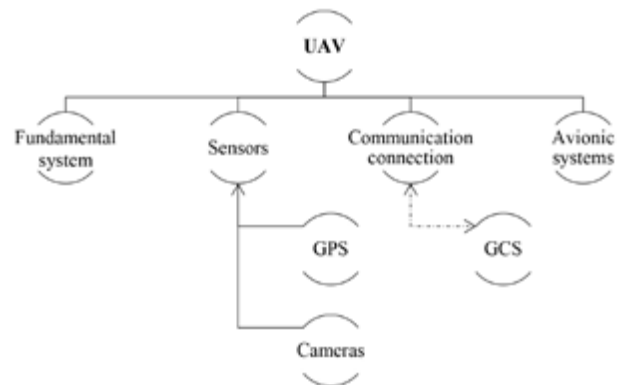


Figure 1. Simplified model of the basic elements of a UAV

The **fundamental system** connects all UAV elements: as Hartman and Steup (2013) effectively said, '[i]t may be considered an UAV "operating system"'. By controlling the other elements, the fundamental system permits the incorporation of other components; for instance, ISR UAVs' *sensors* usually include cameras and GPS (Hartman & Steup, 2013).

**Avionic systems** include all elements contributing to flight capability and allow the received commands to be translated into effective directives for the functioning of e.g. the engine (Hartman & Steup 2013).



The **communication connection** in UAVs can be, for evident reasons, wireless only. Hartman and Steup (2013) classified it into two categories: 'a) direct, line-of-sight (LOS) communication and b) indirect – mostly – satellite communication (SATCOM)'. For the purposes of this article, I am later going to focus more on the former case, as it is the one used most often in off-the-shelf lightweight UAVs.

Although some newer UAV models can operate autonomously, small off-the-shelf lightweight UAVs are manoeuvred by an operator, which requires a Ground Control Station (GCS). Figure 2 shows a simplified model of the basic elements of a GCS.

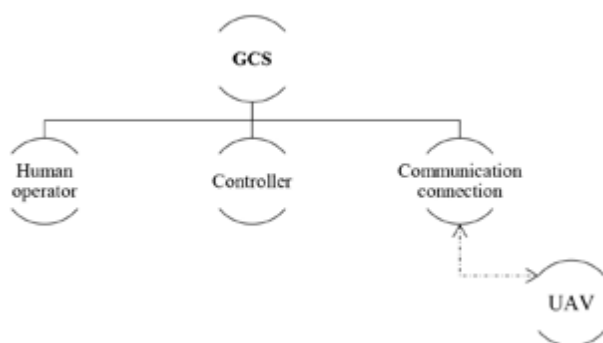


Figure 2. Simplified model of the basic elements of a GCS

The *communication connection* is, as previously mentioned, always wireless in the case of UAVs, and small off-the-shelf lightweight ones are no exception.

Originating from Hartman and Steup's (2013) graphs, I have extrapolated a three-element GCS model that underlines the importance of the *controller*. In the case of off-the-shelf lightweight UAVs, the controller—usually a smartphone or a tablet—is the most important and, at the same time, vulnerable ring of the chain, alongside the communication connection.

### 3. Communication connection vulnerabilities

From an attacker's point of view, the communication connection, being wireless, is the element that is the most difficult to safeguard. It is composed of two flows: a bidirectional one between the UAV and the GCS, and a unidirectional other between the environment and

the sensors (Hartman & Steup, 2013). These links can be exploited in various ways.

---

**From an attacker's point of view, the communication connection, being wireless, is the element that is the most difficult to safeguard. It is composed of two flows: a bidirectional one between the UAV and the GCS, and a unidirectional other between the environment and the sensors.**

---

Because Hartman and Steup (2013) analyse the communication connection in depth, I would only like to drive the reader's attention towards the aforementioned LOS communication. This communication can be implemented under either C-band or Wi-Fi. Both systems utilise omnidirectional antennas (Hartman & Steup, 2013), and are, therefore, more exposed to eavesdropping, especially if the communication is not encrypted. This was the case in 2009, when a terrorist group used a \$26 program, called *SkyGrabber*, to record the video feed off of a US UAV (Gorman, Dreazen & Cole, 2009; Javaid et al., 2012), which had not been encrypted even though the vulnerability had been known to the US armed force for a long time (Arthur, 2009).

### 4. GCS: controller vulnerabilities

The US army considering buying off-the-shelf UAVs brings about a whole new set of problems that had never been previously tackled in the military field: the security of the smartphones and tablets used to control said UAVs. Since the two most popular smartphone OSs, which I will analyse in the following paragraphs, Apple iOS and Google Android, are also used for tablets, and considering that the related issues are exactly the same as in the case of tablets using a Wi-Fi + cellular line, I am going to only use the term *smartphone* for the sake of brevity from now on.

---

**The US army considering buying off-the-shelf UAVs brings about a whole new set of problems that had never been previously tackled in the military field: the security of the smartphones and tablets used to control said UAVs.**

---

#### 4.1. Why commercial smartphones?

BlackBerry phones used to be the go-to device for government workers in many US departments and in the U.K., as they had scored the highest security accreditation. But in 2012, the British government dismissed them in favour of its competitors, Apple and/or Samsung devices (Dalton, 2012), whereas different US governmental agencies moved to either Apple (e.g. the Immigration & Customs Enforcement (Ribeiro, 2012)) or Google Androidrunning devices (e.g. the US Army (Milian, 2012)).

As with off-the-shelf UAVs, commercial devices usually exemplify the most cutting-edge technologies, with the added value of the government not having had to invest considerable sums for their development (Mansfield et al., 2013; Hsu, 2017). Moreover, using mass-market smartphones would be a cost and timeeffective choice, as soldiers are already familiar with the devices if they use similar ones in private (Mansfield et al., 2013).

Using commercial smartphones as GCS for off-the-shelf, lightweight UAVs in ISR missions could bring both advantages and disadvantages. These pocket-sized devices mean that a single soldier can operate the UAV without needing the support of a comrade, hence making utilisation easier in hightension missions, e.g. if the soldiers are under fire or are conducting a surprise operation at night-time. On the other hand, smartphone screens are smaller than a regular laptop's, possibly making all information (realtime images, avionic stats and location, just to name a few) cramped (Mansfield et al., 2013).

---

***Using commercial smartphones as GCS for off-the-shelf, lightweight UAVs in ISR missions could bring both advantages and disadvantages. These pocket-sized devices mean that a single soldier can operate the UAV without needing the support of a comrade, hence making utilisation easier in hightension missions.***

---





## 4.2. Vulnerabilities

The GCS is fundamental for the ISR missions, as it is not only the controller used to manoeuvre the UAV, but acquires data (in the form of images and videos), as well. By targeting the smartphone used as GCS, the attacker can jeopardise the mission itself. In order to do so, attackers can either acquire control of the GCS, or render it inoperative, even creating a denial of service. Fruitful attacks can be performed through communication network, hardware and/or software.

### 4.2.1. Communication Network

Using a smartphone as a GCS necessitates a communication network. As Mansfield et al. (2013) argue, wireless networks in war zones are set up with a stationary base station, which is a tempting target. Making it inoperative equals making the communication network inoperative, as well. In such cases, the soldiers could resort to unsafe civilian networks. Moreover, loss of the communication network can damage, if not disrupt, communication between the GCS and the UAV, making the device uncontrollable as well as allowing for data loss or dispersion, hence jeopardising the mission.

Threats to the communication network include network eavesdropping, spoofing, denial of service and jamming. (Mansfield et al. 2013)

Eavesdropping is the practice of capturing packets of data transmitted over the network and deciphering them (Mansfield et al., 2013). Spoofing consists in the transmission of manipulated data through a network, the access to which has been gained using false credentials (Tippenhauer et al., 2011; Mansfield et al., 2013). Denial of service (DOS) attacks hamper transmission of information between networked agents (Kwon, Liu & Hwang, 2013). In its most primitive form, jamming consists in causing a loss of signal (Giray, 2013)<sup>1</sup>.

<sup>1</sup> I would like to briefly draw attention to the fact that US Marines, as well as other armed forces around the world, have been reportedly equipped with jammers for at least a couple of decades (Schmitt, 1995; Mihelic, 2007; Rogoway, 2014; Military Aerospace Electronics, 2016; US Marine Corps, 2016). Analysing the use of such devices and their impact on UAVs operated by the same actors would far exceed the scope of this article, and is therefore left to further research to be conducted separately, AN.

Communication network vulnerabilities are for the most part solvable through bandwidth allocation and encryption (Mansfield et al., 2013). Bandwidth allocation consists in limiting network access requests to avoid multiple or excessive requests (Guérin, Ahmadi & Naghshineh, 1991; Mansfield et al., 2013). Encryption is the process by which information is codified, so that only authorised agents can decipher it (Skoudis, 2009; Mansfield et al., 2013).

#### 4.2.1.1. Hardware

Smartphones and sensors inside them can be infected by malware software. The malware can enter the device through vulnerabilities in the OS's software or applications; there also exists a risk of malicious software being installed on these devices during the supply chain, which is particularly troublesome to inspect in today's era of transnational companies (Mansfield et al., 2013).

Understandably, the presence of such malware can jeopardise missions and put the soldiers' lives in danger. For instance, by infecting the smartphone's GPS system, the enemy could track the troops' movements, and therefore attack them when they are least expecting it, or provide them with false information.

Mansfield et al. (2013) identify other possible attacks that could impede the correct utilisation of the smartphone as a GCS; among these, I would like to highlight flooding, the practice of overwhelming the device with calls and messages, so that the system is overloaded and/or the human operator is unable to operate the UAV anymore; and battery exhaustion attacks, by means of which the GCS's battery drains exceedingly fast compared to normal battery capacity.

---

***By infecting the smartphone's GPS system, the enemy could track the troops' movements, and therefore attack them when they are least expecting it, or provide them with false information.***

---

An easy way to protect the hardware would be to utilise anti-virus software, which is designed to detect and remove malware immediately.

In war zones, smartphones could more easily fall into the hands of the enemy, thus giving access to information stored on the device. Two solutions to this problem could be the use of passwords and that of encryption, although both can impact the immediacy of use during missions (Mansfield et al., 2013).

#### 4.2.1.2. Software

The OS is the inner foundation of the smartphone, as it controls hardware, sensors and software applications. The enemy, by infiltrating the OS, can acquire complete control over the device and proceed to infiltrate hardware and software applications. This includes acquisition of location, videos and images, as well as conversations (Mansfield et al. 2013). Since the software apps are used to manoeuvre the UAV, accessing them puts the UAV in the hands of the enemy.

As Mansfield et al. (2013) pointed out, smartphones are now vulnerable to the same threats as computers. Alongside the previously-mentioned malware, the software can be infected by viruses such as the 'keylogger' that infected the US UAV fleet's operating computers in a Nevada base in 2011, which registered every tapped key on the keyboard, therefore storing passwords as well (Lawrence 2011; Shachtman 2011).

Below, I will proceed by briefly analysing the three most popular smartphone OSs in light of their application as GCSs in military operations: BlackBerry, Apple iOS and Google Android.

#### 4.2.1.3a. BlackBerry

As explained in the 'Why commercial smartphones?' section, BlackBerry phones were the go-to devices for governmental forces up to 2012, when they lost their position to Apple iOS and Google Android. Even though BlackBerry's devices had been given the highest level of security clearance, and were, therefore, fit to handle classified documents safely (Ribeiro 2012), they were outraced in the technological competition and fell behind. BlackBerry's spot was not single-handedly won by either of its two main competitors: Apple iOS and Google Android



both scored contracts with different US authorities and departments (Kerr, 2012; Milian, 2012; Ribeiro, 2012).

Nonetheless, it may be too soon to carve BlackBerry's epitaph in stone: in 2017, the company won the right to sell its tools to make phone calls and text messages secure through encryption to the US government (Sharp, 2017). So far, however, BlackBerry is still struggling behind its two largest competitors: Apple iOS and Google Android.

#### 4.2.1.3b. Apple iOS

Apple iOS is Apple's unique OS. All updates and alterations to the OS are supervised and executed by the company itself, which allows for reinforced security of devices. On the other hand, all software applications running on Apple iOS need to undergo an App Review, which involves a thorough check and approval by Apple developers (Apple, n.d.). Another limitation involves applications being available only through the Apple store.

Although its devices are used by US governmental agencies, such as the ICE and the Defense Department (Kerr, 2012; Ribeiro, 2012), Apple has been on cold terms with the US government ever since it refused to unlock the San Bernardino shooter's iPhone (Holpuch, 2016; Lichtblau and Benner 2016). If this is considered alongside the difficulty that the US military would have in trying to customise Apple iOS-running products, it comes as no surprise that the Army has been apparently leaning more towards Google Android-running devices.

#### 4.2.1.3c. Google Android

The most popular OS, Google Android's software code is available to the public in order to permit customisations – yet, this liberty equals a downfall in security. Software updates are not as consistently implemented as by Apple, since the customisations have resulted in innumerable variations of the OS itself (Mansfield et al., 2013).

Software applications are available through Google Play, Android's equivalent of the Apple Store, as well as through applications created by developers outside the company.

Although developer's responsibility is in force, applications do not undergo the same scrutiny as in Apple iOS, therefore allowing malicious software to enter the Android sphere undisturbed. In order to tackle this vulnerability concerning both OS and software apps, regular updates seem to be the easiest and most cost-effective solution (Mansfield et al. 2013).

I would like to hereby suggest that the possibility to easily customise this OS, even though it is the cause of its major vulnerabilities, is also its major strength.

Already in 2011, the US Army began testing a modified version of Google Android in order to make it secure enough to handle classified documents (Milian, 2012).

In 2015, the Army's Experimentation Force tested a Samsung Galaxy II-based system: the Nett Warrior Future Initiative, which was a 'special software package' (Cox, 2015). This was also the first time that the InstantEye UAS (Unmanned Aircraft System, a US-only synonym of UAV) was mentioned, as the article states:

"[...] Nett Warrior Future Initiative is equipped with a special software package [...] [s]o a platoon leader can share [...] video streams from a company-level Raven UAS and a platoon-level *InstantEye* UAS with his squad leaders." (Cox 2015, emphasis added)

### 5. InstantEye: the game-changer?

The following year, an article mentioned that, among other UAVs, the InstantEye had been tested by the Army (Hambling, 2016; InstantEye, Robotics 2016). In February 2018, it became official: the US Marine Corps purchased 800 quadcopters from InstantEye Robotics (InstantEye Robotics, 2018) in order to realise what Commandant Robert Neller had envisioned in 2017 (Hsu, 2017). The company worked with the Navy and the Marines to develop the best device for the soldiers' needs (InstantEye Robotics, 2018).

The characteristics of the InstantEye Mk-2 GEN3-A0, the most affordable product from the InstantEye range, include: all-weather and day/night functioning, the possibility

for a single operator to launch it in circa 30 seconds, a twokilometre line-of-sight (LOS) video range, and an endurance of up to 30 minutes (InstantEye Robotics, n.d. a; n.d. b). Moreover, with both UAV and GCS weighing little more than two kilograms (the UAV and the GCS weigh respectively 1.2 and 3.4 lbs (InstantEye Robotics, n.d. b)), it is light enough to be carried by soldiers in their backpacks.

From the GCS's vulnerabilities perspective, it is unknown whether the GCS is a smartphone or a tablet, and if the system runs a modified version of a commercial OS or a specifically-developed one. This is to be expected, as sensitive information such as what OS the GCS is running could compromise the safety of the missions, as I argued previously.

---

***From the GCS's vulnerabilities perspective, it is unknown whether the GCS is a smartphone or a tablet, and if the system runs a modified version of a commercial OS or a specifically-developed one.***

---

Nonetheless, the company has made the following facts public:

The InstantEye Mk-2 GEN3-A0 utilizes a hybrid communication with encrypted, digital link for C2<sup>2</sup> and an analog video link. The aircraft does not store any data onboard, and therefore, there is no data at risk if the aircraft is lost. (InstantEye Robotics n.d. a)

Following my previous analysis, it is clear that the US Marines have solved a few of the afore-mentioned possible problems. First and foremost, the UAV communicates with the GCS via an encrypted connection, substantially disrupting any chance of easy eavesdropping. Moreover, the fact that apparently there is no data storage on board eliminates the threat that, were the UAV to fall in the hands of the enemies, it could provide them with valuable information.

---

<sup>2</sup> Command and control.

Regardless, I would argue that the analogue video link between the UAV and the GCS should be further analysed in order to rule out potential eavesdropping threats.

Because further details on this link are unavailable at the moment, and because this analysis would far exceed the object of this article, I will limit myself to pointing it out.

## 6. Conclusions

The US Army has utilised drones for ISR purposes since the 1980s. At the moment of writing, its UAV arsenal surpasses the 7,000 devices. Yet, the rush towards using such devices will apparently not end any time soon.

In 2016, it was announced that the US Army was considering buying offtheshelf UAVs: to keep up with the developing technology, it seemed best to tap into the ever-growing civilian market. However, because commercial UAVs are often operated through smartphones or tablets, this introduced an entirely new set of vulnerability variables into the picture.

In February 2018, it was announced that the US Navy would purchase 800 InstantEye UAVs for ISR purposes, so as to virtually supply each Marine infantry squad with one. I therefore argued that such a choice, based on the information available at the moment of writing, seemed to be the best solution to prevent most of the previously-mentioned cybersecurity threats. Nevertheless, I would suggest that further research into the InstantEye in-depth specifications, whether and whenever they become official, should be more thorough and complete. Specifically, I would suggest researching the analogue video link that connects the InstantEye UAV to its GCS, as well as the GCS's specifications. ■

## REFERENCES:

- Air Force Technology. (n.d.). *RQ-11B Raven Unmanned Air Vehicle (UAV)*. Retrieved from: <https://www.airforce-technology.com/projects/rq11braven/> [Accessed February 2018]
- Apple. (n.d.). *App Review*. Retrieved from: <https://developer.apple.com/app-store/review/>
- Arthur, C. (2009). SkyGrabber: the \$26 software used by insurgents to hack into US drones. *The Guardian*. Retrieved from: <https://www.theguardian.com/technology/2009/dec/17/skygrabber-software-drones-hacked>
- Chamayou, G. (2014). *Teoria del drone. Principi filosofici del diritto di uccidere*. Roma, Derive Approdi.
- Corrigan, F. (2018). How Do Drones Work and What Is Drone Technology. *DroneZon*. Retrieved from: <https://www.dronezon.com/learn-about-drones-quadcopters/what-is-drone-technology-or-how-does-drone-technology-work/>
- Cox, M. (2015) Soldiers Embrace Smartphone-Based Kit. *Military.com*. Retrieved from: <https://www.military.com/kitup/2015/03/soldiers-embrace-smartphone-based.html>
- Dalton, W. (2012) RIM's BlackBerry phones may lose public sector monopoly. *ITProPortal*. Retrieved from: <https://www.itproportal.com/2012/08/24/rims-blackberry-phones-may-lose-public-sector-monopoly/>
- Elnaggar, M. et al. (2017). Online Control Adaptation for Safe and Secure Autonomous Vehicle Operations. *NASA/ESA Conference on Adaptive Hardware and Systems (AHS)*. Retrieved from: <http://ieeexplore.ieee.org/document/8046365/>
- Giray, S. M. (2013). Anatomy Of Unmanned Aerial Vehicle Hijacking With Signal Spoofing. *2013 6th International Conference on Recent Advances in Space Technologies (RAST)*, Istanbul, 2013, pp. 795-800. Retrieved from: <http://ieeexplore.ieee.org/document/6581320/> [Accessed January 2018]
- Glaser, A. (2017). DJi is running away with the drone market. *Recode*. Retrieved from: <https://www.recode.net/2017/4/14/14690576/drone-market-share-growth-charts-dji-forecast> [Accessed December 2017].



Gorman, S., Dreazen, Y. J., Cole, A. (2009). Insurgents Hack US Drones. *The Wall Street Journal*. Retrieved from: <https://www.wsj.com/articles/SB126102247889095011> [Accessed November 2017].

Guerin, R., Ahmadi, H. and Naghshineh, M. (1991). Equivalent capacity and its application to bandwidth allocation in high-speed networks. *IEEE Journal on Selected Areas in Communications*, vol. 9, no. 7, pp. 968-981, Sep 1991. Retrieved from: <http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=103545&isnumber=3202> [Accessed February 2018].

Hambling, D. (2016). The US Army Wants Tiny Flying Eyes for Every Footsoldier. *Popular Mechanics*. Retrieved from: <https://www.popularmechanics.com/military/research/a20862/the-army-wants-tiny-flying-eyes-for-every-footsoldier/> [Accessed December 2017].

Hartmann, K. & Steup, C. (2013). The Vulnerability of UAVs to Cyber Attacks - An Approach to the Risk Assessment. 2013 5<sup>th</sup> *International Conference on Cyber Conflict*. NATO CCD COE Publications, Tallinn. Retrieved from: <http://ieeexplore.ieee.org/document/6568373/> [Accessed January 2018]

Holpuch, A. (2016). Tim Cook says Apple's refusal to unlock iPhone for FBI is a 'civil liberties' issue. *The Guardian*. Retrieved from: <https://www.theguardian.com/technology/2016/feb/22/tim-cook-apple-refusal-unlock-iphone-fbi-civil-liberties> [Accessed February 2018]

Hsu, J. (2017). The Military May Soon Buy the Same Drones You Do. *Wired*. Retrieved from: <https://www.wired.com/2017/01/military-may-soon-buy-drones-home/> [Accessed December 2017].

InstantEye Robotics (2016). *InstantEye in the News*. Retrieved from: <https://instanteyerobotics.com/uncategorized/national-defense-marine-corps-experimenting-with-new-drones/> [Accessed February 2018].

(2018). United States Marine Corps Orders 800 InstantEye Systems. Retrieved from: <https://instanteyerobotics.com/uncategorized/united-states-marine-corps-orders-800-instanteye-systems/>

(n.d. a) *InstantEye Mk-2 GEN3*. Retrieved from: <https://>

[instanteyerobotics.com/products/gen3/](https://instanteyerobotics.com/products/gen3/)

(n.d. b) *InstantEye Mk-2 GEN3-A0 sUAS Specification Sheet*. Retrieved from: <https://instanteyerobotics.com/wp-content/uploads/2017/11/InstantEye-Mk-2-GEN3-A0-v2.3-11-20-17.pdf>

Javaid, A. Y., Sun, W., Devabhaktuni, V. K., Alam, M. (2012). Cyber Security Threat Analysis and Modeling of an Unmanned Aerial Vehicle System. 2012 *IEEE Conference on Technologies for Homeland Security (HST)*, Waltham, MA, 2012, pp. 585-590. Retrieved from: <http://ieeexplore.ieee.org/document/6459914/>

Javaid, A. Y., Sun, W., Mansoor, A. (2013). UAVSim: A Simulation Testbed for Unmanned Aerial Vehicle Network Cyber Security Analysis. *Globecom 2013 Workshop - Wireless Networking and Control for Unmanned Autonomous Vehicles*. Retrieved from: <http://ieeexplore.ieee.org/document/6825196/>

Kwon, C., Liu, W., Hwang, I. (2013). Security Analysis for Cyber-Physical Systems against Stealthy Deception Attacks. 2013 *American Control Conference (ACC)*. Retrieved from: <http://ieeexplore.ieee.org/document/6580348/>

Lawrence, C. (2011). Virus infects program that controls US drones. *CNN*. Retrieved from: <http://edition.cnn.com/2011/10/10/us/drone-program-virus/index.html> [Accessed December 2017].

Lichtblau, E. and Benner, C. (2016). Apple Fights Order to Unlock San Bernardino Gunman's iPhone. *The New York Times*. Retrieved from: <https://www.nytimes.com/2016/02/18/technology/apple-timothy-cook-fbi-san-bernardino.html>

Karpowicz, J. (2018). 8 Commercial Drone Predictions for 2018. *Commercial UAV Expo*. Retrieved from: <https://www.expouav.com/wp-content/uploads/2017/12/8-Commercial-Drone-Predictions-for-2018.pdf>

Kerr, D. (2016). Defense Department drops exclusive contract for BlackBerry. *CNET*. Retrieved from: <https://www.cnet.com/news/defense-department-drops-exclusive-contract-for-blackberry/>

Kim, A. et al. (2012). Cyber Attack Vulnerabilities Analysis for Unmanned Aerial Vehicles. *American Institute of Aeronautics and Astronautics*. Retrieved from: <https://arc.>



[aiaa.org/doi/abs/10.2514/6.2012-2438](http://aiaa.org/doi/abs/10.2514/6.2012-2438)

Mansfield, K. et al. (2013). Unmanned Aerial Vehicle Smart Device Ground Control Station Cyber Security Threat Model. *2013 IEEE International Conference on Technologies for Homeland Security (HST)*, Waltham, MA, 2013, pp. 722-728. Retrieved from: <http://ieeexplore.ieee.org/document/6699093/>

Mihelic, P. (2007). Jamming systems play secret role in Iraq. *CNN*. Retrieved from: <http://edition.cnn.com/2007/TECH/08/13/cied.jamming.tech/>

Milian, M. (2012). US government, military to get secure Android phones. *CNN*. Retrieved from: <https://edition.cnn.com/2012/02/03/tech/mobile/government-android-phones/index.html>

Military Aerospace Electronics (2016). Backpack jammers help Marines counter roadside bombs, disrupt enemy communications. *Military Aerospace Electronics*. Retrieved from: <https://www.militaryaerospace.com/articles/print/volume-27/issue-1/product-applications/backpack-jammers-help-marines-counter-roadside-bombs-disrupt-enemy-communications.html>

Morante, S., Victores, J. G. & Balaguer, C. (2015). Cryptobotics: why robots need cyber safety. Retrieved from: <https://www.frontiersin.org/articles/10.3389/frobt.2015.00023/full> [Accessed January 2018]

Pullen, J. P. (2015). This Is How Drones Work. *Time*. Retrieved from: <http://time.com/3769831/this-is-how-drones-work/>

Ribeiro, J. (2012). BlackBerry loses government contract to iPhone. *PCWorld*. Retrieved from: <https://www.pcworld.com/article/2012862/blackberry-loses-government-contract-to-iphone.html>

Rivera, E., Baykov, R., Gu, G. (2014). A Study On Unmanned Vehicles and Cyber Security. Retrieved from: <https://pdfs.semanticscholar.org/>



ANALYSIS

# QUANTUM TECHNOLOGIES AND STANDARDIZATION



**TOMASZ MAZUR**

Manager of three Sectors in Standardization Department of Polish Committee for Standardization: Information Technology and Communications Sector, Defence and Public Security Sector, Nanotechnology and Innovation Sector; Microsoft Certified System Administrator – specialization: Security

**The so-called second quantum revolution will lead to a wave of new technologies that will create many new businesses. It will give us devices with fundamentally superior performance and capabilities for sensing, measuring, imaging, computing as well as for communication and simulation.**

Some are already starting to be commercially exploited. Others may still require years of careful research and development. Universal quantum computing is considered to be more than 10 years to possibly even several decades away, but special purpose machines, for simulation in particular, may be possible in less than 10 years.

Realising that quantum technologies will be an important game-changer, the European Commission has launched the Quantum Technology Future and Emerging Technologies (FET) Flagship programme with an overall budget of EUR 1 billion [4], with the aim of turning Europe's promising research results into concrete technological opportunities that can be taken up by the industry.

'Technologies based on the laws of quantum mechanics, which govern physics on an atomic scale, will lead

to a wave of new technologies that will create many new businesses and help solve many of today's global challenges.' This sentence from 'Quantum Manifesto', a paper produced in May 2016 by a team of European experts, illustrates how high the expectations are when it comes to the second quantum revolution. Previously, applications based on quantum behaviour led to the emergence of transistors and lasers, but the second quantum revolution will lead to new devices with different and sometimes revolutionary characteristics.

---

***Technologies based on the laws of quantum mechanics, which govern physics on an atomic scale, will lead to a wave of new technologies that will create many new businesses and help solve many of today's global challenges.***

---

## Examples of applications

- Quantum computing devices**  
 Quantum computers using quantum bits, or qubits, will process certain types of problems more effectively than conventional digital computers. They will offer new and powerful methods of solving problems which would take infinitesimal time to solve for conventional computers.
- Quantum-enhanced imaging**  
 Quantum-enhanced imaging systems will provide new opportunities in areas such as imaging and range finding in low light, or low-cost multi-spectral imaging technologies. Artificial Intelligence (AI) is already used in some of these areas, but quantum technologies will provide further enhancements with applications in scientific devices like microscopes and telescopes used in defence and environmental monitoring. Quantum-enhanced imaging could also be applied to medical imaging devices but after appropriate regulatory approval.
- Quantum gravity sensing devices**  
 In the foreseeable future, we should witness the emergence of quantum gravity field and gradient sensors. They will be used to create 3D maps of the density of the surroundings, making huge impact on the world's construction and mining sectors. These future sensors will allow virtual penetration of the ground, using gravity as means of detection and identification of buried objects that are undetectable for the currently used devices.
- Quantum secure communications**  
 Nowadays, public key cryptography is based on the assumption that some mathematical operations are too difficult to solve by widely available digital computers. That may change when processing power of the future computers will rise (according to Moore's law or faster), making current cryptographic methods vulnerable to an attack. Quantum secure communication systems using effects like quantum entanglement might be a solution for secure sensitive data transmissions.

- Quantum acceleration and navigation devices**  
 Quantum inertial measurement units (IMU) will offer a dramatic improvement of existing IMUs. These future devices will allow navigation by measuring acceleration and rotation, without the need of connecting to GPS or other satellite positioning systems. These can enable precise indoor, subterranean or underwater navigation.
- Quantum timing devices**  
 Next-generation atomic clocks and quantum communication systems will enable the creation of accurate timing and navigation devices. Today, timing for many applications comes from satellite signals in global satellite positioning systems. It is an important part of our economy and other aspects of life. Quantum timing devices will provide very precise timing within a device itself, making it independent of satellite's or any other external signals.

## The role of standardization

Quantum technologies are relatively new and immature but with continuous development they will slowly create new opportunities for entrepreneurship. As with every industrial revolution, a need for standardization will follow that growth.

Standards are useful enablers of future technology development, giving confidence and commonality in both well-developed and emerging markets. Introducing standards for many applications of quantum technologies will be crucial to delivering significant market uptake.

---

***Quantum technologies are relatively new and immature but with continuous development they will slowly create new opportunities for entrepreneurship.***

---

In terms of market access, quantum cryptography is currently the most developed subfield of the new generation of quantum technology, and there are companies specialising in quantum cryptography. The European Telecommunications Standards Institute (ETSI) is already working on standards for quantum cryptography in its Industry Specification Group on Quantum Key Distribution (ISG/QKD). This ISG was established following



the work of the SECOQC FP6 project [4]. Quantum Key Distribution is based on the purely physical quantum characteristics of transmitted photons and utilise one of the most unusual principles governing the quantum realm called 'the observer effect'. This principle stipulates that the observation/measurement of a quantum object affects its properties. The above allows an encryption key to be sent securely over the network, making any attempt of interception or espionage detectable, ultimately resulting in the invalidation of the key.

There are two national technical bodies of the Polish Committee for Standardization (PKN) cooperating with ETSI: Technical Committee 11 'Telecommunications' and Technical Committee 172 'Personal Identification, Electronic Signature, Smart Cards and Related Systems'. The scope of Committee 172 includes standards for the generation and handling of encryption keys as well as electronic signatures with some examples listed below:

PN-EN 419211-1:2014-12 Protection profiles for secure signature creation device – Part 1: Overview

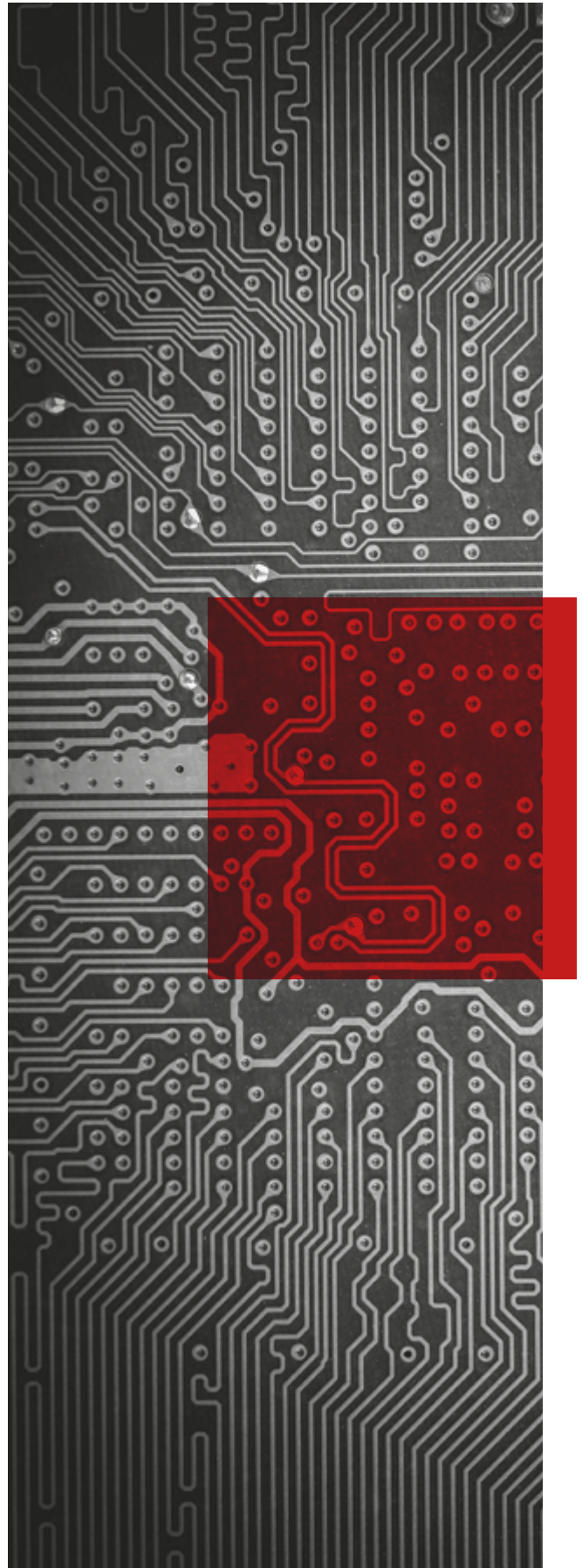
PN-EN 419211-2:2013-11 Protection profiles for secure signature creation device – Part 2: Device with key generation

PN-EN 419211-3:2014-02 Protection profiles for secure signature creation device – Part 3: Device with key import

PN-EN 419211-4:2014-02 Protection profiles for secure signature creation device – Part 4: Extension for device with key generation and trusted channel to certificate generation application

PN-EN 419211-5:2014-02 Protection profiles for secure signature creation device – Part 5: Extension for device with key generation and trusted channel to signature creation application

PN-EN 419211-6:2014-12 Protection profiles for secure signature creation device – Part 6: Extension for device with key import and trusted channel to signature creation application





As these standards do not encompass the aspects of quantum cryptography, further advancements in this field will force their revision or supersession as well as the creation of entirely new standardization documents.

The development of cryptographic algorithms, which will be capable of resisting attacks by 'quantum computers', is another prerequisite for secure communications. As forecasted, quantum computers will be able to easily break almost all public key cryptography encryption available today, giving rise to what is called 'Post Quantum Cryptography'. Again, ETSI is involved with the Industry Specification Group (ISG) on Quantum-Safe Cryptography (QSC). QSC is also within the scope of the Joint Technical Committee of International Organization for Standardization (ISO) and International Electrotechnical Commission (IEC) ISO/IEC JTC 1/SC 27/WG 2 'Cryptography and security mechanisms', although there is currently no work item there with such a title.

PKN's Technical Committee 182 'Security of Information in ICT Systems', entered into cooperation with Working Group 2 in 2012 and delegated a group of experts who attended several meetings of the group, including the most recent one that took place in Wuhan, China, on 9 April 2018.

While there is no intention to start any standardization activity that would duplicate the effort made within ETSI, there are good reasons to believe that standardisation should play a role in all aspects of quantum technologies. Whenever new technologies are to be brought to the market, it is important to set quality and performance requirements for them, and to create trust in the innovative solutions. Standards will play an important role here. Also, quantum technology-enabled components/devices will not stand on their own but will be integrated into the existing products/systems. Product manufacturers will demand quantum technologies in the form of subsystems. The requirement for interoperability will raise the need for standardization.

---

***Whenever new technologies are to be brought to the market, it is important to set quality and performance requirements for them, and to create trust in the innovative solutions.***

---

The Commission's Staff Working Document on Quantum Technologies stresses that we will witness the emergence of supply chains of quantum enabling technologies: 'There are many opportunities for new as well as existing companies to sell quantum components and sub-systems at first to the academic market, and then to the growing quantum industry within emerging supply chains of quantum enabling technologies. Examples of such technologies are cryogenic systems, single photon sources and detectors, entangled photon pair sources, materials (e.g. superconducting junctions), material processing techniques, quantum algorithms, protocols and software. In the longer term there will be routine need for miniaturized plug-and-play quantum devices that today require bulky laboratory setups under carefully controlled conditions. In addition, there are multiple spin off markets for cutting edge photonic, electronic or opto-mechanical devices.'

Therefore, standardization in support of these enabling technologies will also be needed. ■

## REFERENCES

---

CEN/CENELEC Management Centre correspondence.

European Commission (2016). Commission Staff Working Document on Quantum Technologies accompanying the Document Communication from the Commission to the European Parliament, The Council, The European Economic and Social Committee and the Committee of the Regions, European Cloud Initiative Building a Competitive Data and Knowledge Economy in Europe. Retrieved from: <https://ec.europa.eu/digital-single-market/en/news/commission-staff-working-document-quantum-technologies>

De Touzalin, A., Marcus, C., Heijman, F., Cirac, I., Murray, R., Calarco T. (2016). Quantum Manifesto. Retrieved from: <http://quop.eu/manifesto>

Lewis, A., Kraemer, M., Travagnin, M. (2016). Quantum Technologies: implications for European Policy. Retrieved from: <https://ec.europa.eu/jrc/en/publication/eur-scientific-and-technical-research-reports/quantum-technologies-implications-european-policy-issues-debate>

ANALYSIS

# BETWEEN CYBER AND PHYSICAL WORLDS: SECURE ENDPOINT DEVICES AS THE KEY INTERFACE FOR A BLENDED REALITY FUTURE



**GIULIA PASTORELLA, PHD**

Giulia is Cybersecurity and Data Policy Lead in HP's Government Relations Global Strategy Program. Based in Brussels, she has been with HP since 2015, being responsible for Government Relations in the UK, Italy and the EU. She works closely with HP Labs in Bristol doing cybersecurity research. Before joining HP, Giulia worked in public affairs in a variety of sectors, including think tanks. She holds a PhD and Master's degree from the London School of Economics in European Affairs and a Bachelor of Arts from Oxford University in Philosophy and Languages. Giulia was nominated one of the Forbes 30 under 30 most influential people in Europe for policy.



**SIMON SHIU, PHD**

Simon is currently head of the Security Lab at HP Inc. He has been with HP Labs for over 20 years and has led a number of research teams and published several academic and professional articles on a wide range of topics spanning secure hardware, trusted infrastructure, cloud computing, audit, governance, and the economics of information security. Simon has always had a strong external presence working directly with customers, leading HP's participation in EU and UK government-funded research collaborations, and working with several of the UK universities that focus on security. Since 2015, Simon has led the Security Lab which has made HP a leader in cyber resilient endpoint devices. A PhD graduate in computer science from Durham University, he serves on several academic advisory committees and is a member of the Institute of Information Security Professionals (M.Inst.ISP).

Cybersecurity is constantly in the news. Barely a day passes without a new story about yet another cyberattack. In addition to espionage, theft and misinformation, we see an increasing trend towards destructive attacks. Such attacks go back a long way before Stuxnet that targeted the Iranian nuclear facility, but the trend has continued and grown ever since. One mainstream example is the Mirai virus that quietly compromised thousands of IoT devices and then used this botnet to create extremely large scale distributed denial of service (DDOS) attacks. The Mirai attack exploited consumer devices, but commercial enterprises struggle

to defend themselves from attacks, too. In 2017, we saw a wave of ransomware attacks that encrypted data on PCs, not to mention the fact that there were also versions of the malware that went a step further by corrupting firmware and causing significant damage to devices.

In all these examples, the cybersecurity of the physical-digital system was undermined by exploiting an 'edge' device and its corresponding device ecosystems. Edge devices define the boundary between our physical and digital worlds and are therefore the cornerstone of our

future Blended Reality world<sup>1</sup>. This article will argue that the importance of edge devices is growing, and so is the attention they are getting from hackers. Governments around the world, too, are increasingly realising the importance of device security at the deepest level and are designing policies to incentivise industry to take action. For instance, a recent roundtable organised by the UK Department for Culture, Media and Sport and the National Cyber Security Centre on firmware security highlighted a growing need for simplifying methods end-users can use to keep their devices secure and up to date, thus reducing the burden on business and the general public.

---

***Edge devices define the boundary between our physical and digital worlds and are therefore the cornerstone of our future Blended Reality world***

---

Overall, the negligence of device security is increasing the likelihood of disastrous consequences. For our future to be truly a Blended Reality one and free from being constantly under threat of disruption, we need to start securing all devices now.

### **Edge devices, the cornerstone of a Blended Reality world**

The move towards Blended Reality is manifest in all sectors, from healthcare to manufacturing, from transportation to the home appliance industry, from agriculture to critical utility infrastructures. In all these areas, endpoint devices are the first line of defence for the data and resources we care about. They are the interface between the physical and the digital world, and a prime target for cyberattacks today, and for years to come. Existing technologies such as PCs, scanner-printer-copiers, 3D printers, immersive devices, sensors and actuators sit between people and cyberspace, providing novel on-ramps and off-ramps between these domains. Paradoxically, they are both the fundamental element and a potential weak link in new Blended Reality scenarios.

---

<sup>1</sup> **'Blended reality'** is a term first used by the futurist think tank, the Institute for the Future (ITF). The ITF envisioned it as a tech-enabled sixth sense, which will be worn or maybe even implanted into our bodies and interfaced with our computers.

---

***Endpoint devices are the first line of defence for the data and resources we care about. They are the interface between the physical and the digital world, and a prime target for cyberattacks today, and for years to come.***

---

The fusion of our physical and digital worlds creates particular challenges for cybersecurity. The number and types of devices used by people or deployed to interact with the physical world grows rapidly, often without applying well-established IT security best practices. This results in many new products reaching the market with gaping vulnerabilities. Unfortunately, a device with poor security design or poor management can open up a whole network to attack. In consequence, malicious actors have a larger attack surface than ever before.

### **The threat landscape**

In parallel to the rapidly evolving landscape of cyber-physical interaction, the landscape of cybersecurity threats is also experiencing a dramatic shift. The accelerated innovation path towards Blended Reality increases both the supply and demand for cyberattacks. As our societal and economic dependency on technology grows, so does the motivation for malicious groups to use cyberattacks for economic gain, activism, espionage, and propaganda. These groups are increasingly professional, more aggressively funded, and better equipped. Because of a rising number of devices in circulation, we are also seeing a rise in firmware attacks. These attacks target the software embedded in hardware and, if successful, provide an attacker with control over an entire system. What is even more worrisome, we are seeing an accelerating trend in destructive attacks that target low-level firmware to disable hardware devices and render them inoperable on a large scale. In a nutshell, cyberattacks are increasingly trying to introduce malware into device's firmware to eavesdrop, monitor, and even attempt to disable computing infrastructures. This new trend undermines a safe evolution towards Blended Reality and therefore calls for coordinated efforts.

Governments are taking action in this respect. The European Union Cybersecurity Act (European Commission, 2017<sup>2</sup>) aims at ensuring minimum levels of security for connected devices through a voluntary certification scheme. Other countries, such as Germany or the UK, are following a similar path through the Code of Practice (Department for Digital, Culture, Media & Sport, 2018<sup>3</sup>) and specific certification schemes. Across the Atlantic, too, the Internet of Things (IoT) Cybersecurity Improvement Act, which was proposed in 2017, seeks to provide minimal cybersecurity operational standards for Internet-connected devices purchased by federal agencies. The list could continue.

*As our societal and economic dependency on technology grows, so does the motivation for malicious groups to use cyberattacks for economic gain, activism, espionage, and propaganda.*



<sup>2</sup> Drafted by the Commission, the text is still going through the legislative process.

<sup>3</sup> Draft is still being finalised.

At HP, we have long considered endpoint edge devices the frontline of the cybersecurity battle ground. We think that inventing security solutions for key future technology disruptions that will enable a Blended Reality future is one of the key challenges that companies around the globe are facing today.

### **HP's focus on cyber-resilient devices: an answer to present and future Blended Reality challenges**

Security teams in large organisations put a lot of energy into deploying, configuring and managing security mechanisms that work at the software (operating system and above) layer. These mechanisms are important, but it is equally vital to recognise that sophisticated attacks will always find ways to compromise trusted software to hide or persist on a platform. Hardware provides the foundation for more robust mechanisms that the OS and security critical software can rely on. This is why security needs to be designed and built in from the beginning and from hardware up.

As a longstanding manufacturing company, HP has realised early on that the cybersecurity of edge devices – and firmware in particular – will become one of the industry's leading challenges. For over 25 years, HP Labs has worked to improve cybersecurity capabilities in computing systems. During this time, cyber threats have transformed into a major priority for all industries. From trusted systems design to the economics of security, HP Labs has a long track record of industry leadership with security innovation. Today at HP Inc., cybersecurity remains central to our commitment to delivering the most secure products, leading institutional security innovation, and inventing security solutions for key future technology disruptions such as 3D printing, the digitisation of manufacturing, and the emerging cyber-physical world around us.

Most importantly, in today's threat landscape, the security profession is accepting the axiom that given enough resources, an attacker will eventually be successful. This means designing not only security protections, but also mechanisms that automatically detect when protections fail and help recover devices or infrastructure to a good state, without human intervention and at scale. HP has



been leading the industry in designing systems and devices that incorporate hardware-enforced security from the lowest level of firmware and working up through the software stack and management solutions.

---

***In today's threat landscape, the security profession is accepting the axiom that given enough resources, an attacker will eventually be successful.***

---

Design for cyber-resilience is meant to ensure that devices are not only built with protections, but also with reliable mechanisms to detect successful attacks, and recover from them. This is a model that has already been embraced across HP's business PC and Print products, using robust hardware foundations to achieve resilience. This model will be deployed in future edge devices to ensure they are not the weakest link in the Blended Reality world.

### **Securing future technologies: an example from the digital manufacturing sector**

HP's Security Lab pursues original system security research to ensure that we deliver safe and assured products, services and experiences, and lead the industry in raising the bar in cybersecurity. To that end, we focus on endpoint security with three core research themes: device security research, infrastructure security, and security management research. As part of the device security research, we innovate and continue to raise the bar in how we co-design hardware and software for cyber resilient platform architectures. With respect to infrastructure security, we design secure device-to-device and device-to-cloud interactions that will provide users with safe and seamless experience. In the context of security management research, we focus on attack detection and manageable remediation across large fleets of devices and future endpoint ecosystems.

---

***Our security research team is now developing its own techniques for simulating malware behaviour, allowing us to test our protection and detection solutions against possible future malware behaviours, even before our adversaries develop them.***

---

We have created our own isolated Malware Lab wherein we investigate pieces of malicious software. This lets us experiment with malware in a contained environment to better understand our adversaries, and test our research approaches to detecting, mitigating, and recovering from real-world attacks. We also want to know which anti-malware solutions might work against the yet unidentified malware. Our security research team is now developing its own techniques for simulating malware behaviour, allowing us to test our protection and detection solutions against possible future malware behaviours, even before our adversaries develop them.

Since HP is a technology company that primarily sells endpoint devices, related services and solutions, our research will help secure key future technologies such as the 3D ecosystems that promise to revolutionise manufacturing. One area that is of particular relevance to the new Blended Reality world and therefore needs to be built and maintained secure is the digitisation of manufacturing through 3D printing.

For example, we are researching the security innovations needed for 3D printing technology to revolutionise manufacturing. These range from cybersecurity research for MultiJet Fusion machines – our 3D printers themselves, to researching the design of secure workflow capabilities to ensure the maintenance of key security properties in digital designs until they become physically printed objects. This will be key to ensuring that the physical and mechanical properties of a 3D-printed part can be trusted within a securely digitised distributed manufacturing ecosystem. As Paul Benning, Ph.D., HP Fellow and 3D Print Chief Technologist reminds us:

*Cybersecurity is important to the success of the HP 3D Print business and the manufacturing transformation HP is driving. We are working closely with the Security Lab to deliver a secure 3D ecosystem and to develop valuable security innovation for future digitized supply chains that will transform manufacturing.*

## Conclusions: secure devices for a secure Blended Reality future

While edge devices are important, at HP we are aware that cybersecurity for Blended Reality can only be addressed comprehensively by working in partnership with others. We have come to the realisation early on that a single layer of defence will not suffice anymore, especially as we are progressively moving to a Blended Reality future in which interactions between connected objects are the norm. If we simply keep building ever-higher walls, the increasingly well-funded professional criminal organisations will sooner or later find a way through. Instead, we need multiple security mechanisms built in at the deepest level of our computing devices and infrastructures and offering resilience against cyberattacks. We also need to manage security in a cost-effective manner. Security architectures and innovation must come at an affordable cost and match user needs. This makes end customers important partners in defining research approaches and priorities. Our work takes us beyond HP to global standards bodies and into collaborations with industrial and academic partners, with whom we join forces to advance the cybersecurity state-of-the-art technology and move our industry forward towards a safer Blended Reality future.

Working with industry colleagues, collaborating on industry standards to help raise the bar in cybersecurity across the world is a necessary enabler of a sustainable approach to a secure Blended Reality. There is also a role for government in expanding the ecosystem to include a wide range of stakeholders, identifying and highlighting good practice, and providing cyber security advice and guidance for a wide range of audiences.

As we are inventing our exciting new Blended Reality future, we also need to solve cybersecurity challenges of a new sort. More and more devices are collecting data to change or configure the physical world. With this being said, the security of endpoints and their ecosystems will only become more critical to the cybersecurity of any organisation, regardless of whether it operates in logistics, healthcare, transportation, manufacturing or other industries. Hardware provides the foundation and low-level security that is increasingly critical to any operating system,

or software security solution, on and around endpoints. In this context, choosing the right device is already a security decision. ■

## REFERENCES

---

1. European Commission (2017). Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on ENISA, the "EU Cybersecurity Agency", and repealing Regulation (EU) 526/2013, and on Information and Communication Technology cybersecurity certification ("Cybersecurity Act"). Retrieved from: [http://www.europarl.europa.eu/RegData/docs\\_autres\\_institutions/commission\\_europeenne/com/2017/0477/COM\\_COM\(2017\)0477\\_EN.pdf](http://www.europarl.europa.eu/RegData/docs_autres_institutions/commission_europeenne/com/2017/0477/COM_COM(2017)0477_EN.pdf)
2. Department for Digital, Culture, Media & Sport (2018). Secure by Design: Improving the cyber security of consumer Internet of Things. Retrieved from: [https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment\\_data/file/686089/Secure\\_by\\_Design\\_Report\\_.pdf](https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/686089/Secure_by_Design_Report_.pdf)

# WHERE CYBER MEETS SECURITY



**CYBERSEC  
EXPO 2019**

**17-18.01.2019**

**GlobalEXPO Warsaw**

**CYBERSEC**

**GET IN TOUCH**

Sales Office +48 618 473 755, [info@cybersecexpo.eu](mailto:info@cybersecexpo.eu)



ANALYSIS

# INFORMATION SHARING FOR THE MITIGATION OF HOSTILE ACTIVITY IN CYBERSPACE: COMPARING TWO NASCENT MODELS (PART 1)



DEBORAH HOUSEN-COURIEL

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

## 1. Introduction: Defining the Threat and the Opportunity

### 1.1 Overview

Information sharing (IS) among private sector and governmental entities can serve as an effective tool for bolstering cybersecurity and mitigating damage caused by hostile cyber incidents. It does so by bridging gaps due to information asymmetries between attackers and their targets, identifying the vulnerabilities of targeted organizations and the means to quickly mitigate these exposures, and reinforcing best practices for cyber defence, both in real time and in the long term. Yet in the absence of regulation mandating IS, private sector actors may be reluctant to share information voluntarily. Even when government regulation requires IS, private sector actors' participation may not be optimal. They attribute

several drawbacks to current sharing platforms, including imperfect trust relationships among participants; a lack of transparency regarding the efficiency and confidentiality of IS measures; exposure to legal liability with respect to the information shared (i.e., protected personal data); and operational and personnel costs.

In this two-part article, we briefly analyse and compare two current IS developments in light of these overarching concerns. The first is the 2016 EU Network and Information Systems Directive (NIS) that came into effect in May 2018<sup>1</sup>, followed by Israel's Financial Cyber and Continuity Center (IFC3) established in January 2017 (Ministry of Finance, 2017, September 4). The NIS is a mandatory regulatory framework that applies to all EU member states and,

<sup>1</sup> Directive 2016/1148 concerning Measures for a High Common Level of Security of Network and Information Systems Across the Union, 2016 O.J. (L194) 1 [hereinafter NIS].



once fully transposed, will apply to a broad spectrum of organizational sectors which these states will designate the operators of essential services (i.e., energy, transport, water supply) and digital service providers<sup>2</sup>. Under the NIS, member states themselves are required to exchange information as part of their strategic cooperation for bolstering cybersecurity; and domestic operators and providers, including private sector actors, are required to share information through a regulatory regime of incident notification. In contrast to the NIS model, the IFC3 is a national IS platform, sector-specific and voluntary. Under both frameworks the information sharing *praxis* is currently evolving.

This article proposes that, as they are increasingly implemented, each model holds insights for the functioning of its counterpart. In the first part of the article we review IS as an element of jurisdictional cybersecurity, whether the jurisdiction is sectoral, national, or transnational. In the second part, we analyse and compare the information sharing measures and modalities of the NIS and the IFC3 as well as some of the issues that emerge from this comparison of two nascent IS platforms. The conclusion points to two future challenges for information sharing measures, whether mandated or voluntary: the special case of IS posed by responsible disclosure of cyber vulnerabilities; and the imperative to include new stakeholders, such as individual end-users of cyber products and services, in innovative ways that ensure trusted IS relationships are maintained.

## 1.2 Information Sharing as an Element of Cybersecurity

As hostile cyber incidents continue to escalate globally in their prevalence, disruptiveness, and financial costs, information sharing to mitigate the impact of such hostile activity in cyberspace is one of the most widely advocated measures for increasing organizational, national, and global

<sup>2</sup> Although the deadline for NIS transposition was set for 9 May 2018, as of this writing eleven of the 28 member states have proceeded with this process (Cyprus, Czech Republic, Estonia, Finland, Germany, Italy, Malta, Slovakia, Slovenia, Sweden, and the UK). See European Commission. (2018, May 4); and European Commission. (2018, July 19).

cybersecurity among vulnerable organizations<sup>3</sup>. Although not the sole means of closing organizational gaps, nor by any means a blanket remedy, it is relied upon as a key measure for bolstering cybersecurity<sup>4</sup>. Thus, in situations in which hostile cyber incidents have spread rapidly around the globe, such as in the May 2017 WannaCry ransomware attack, real-time IS has effectively supported coordinated responses among a wide spectrum of stakeholders, including both states and private sector actors across many regulatory jurisdictions (Chabrow, 2017, November 14; and *WannaCry Ransomware Attack...*, n/d). Moreover, strategic IS, such as that supported by Information Sharing and Analysis Centres (ISACs), can leverage the best practices of diverse stakeholders for preparedness, response, and resilience in the long term (ENISA, 2017).

---

***As hostile cyber incidents continue to escalate globally in their prevalence, disruptiveness, and financial costs, information sharing to mitigate the impact of such hostile activity in cyberspace is one of the most widely advocated measures for increasing organizational, national, and worldwide cybersecurity among vulnerable organizations.***

---

In particular, IS can mitigate inherent informational asymmetries with respect to cyber risk assessment and response in the rapidly-changing threat environment of cyberspace<sup>5</sup>. The inherently global nature and scope

<sup>3</sup> On the escalation of cyber threats, see World Economic Forum. (2018). IS for increased cybersecurity is widely seen as critical across all sectors and industries (see Deloitte and Fraunhofer. (2013)). "Cybersecurity" is defined for present purposes as the process of implementing actions for the identification, prevention, mitigation, investigation, and handling of cyber threats and incidents in a digitized network; for the reduction of their effects on the network; and for the network's increased resilience in the wake of such threats and incidents.

<sup>4</sup> "Cyber threat information sharing is not a cure-all solution, but it is a critical step toward improving cyber defenses. The benefits of information sharing, when done correctly, are numerous. Sharing enables organizations to enhance their cyber defenses by leveraging the capabilities, knowledge, and experience of a broader community. It can provide better situational awareness of the threat landscape, including a deeper understanding of threat actors and their tactics, techniques, and procedures (TTPs), and greater agility to defend against evolving threats. It can improve coordination for a collective response to new threats and reduce the likelihood of cascading effects across an entire system, industry, sector, or across sectors." (Zheng and Lewis, (2015), at 1).

<sup>5</sup> These asymmetries may exist at several levels: as between the hostile attacker and the vulnerable organization; as between governmental actors and private sector actors; and among private sector actors possessing varying risk assessment capabilities (Gibbs, Shanks, and Lederman, 2005).

of cyber activities, including hostile incidents, means that cyber threats, risks and exposures are interconnected. Thus, effective inter-organizational and cross-boundary responses depend upon reliable, relevant, and timely information sharing. The operative benefits of IS are manifested most clearly around hostile cyber events or incidents<sup>6</sup>, yet information sharing is also crucial as an ongoing activity, independent of any specific cyber event. Analyst Sean Barnum explains the strategic criticality of IS among private sector entities:

'[N]o organization in and of itself has access to an adequate scope of relevant information for accurate situational awareness of the threat landscape. *The way to overcome this limitation is via sharing of relevant cyber threat information among trusted partners and communities.* Through information sharing, each sharing partner can potentially *achieve a more complete understanding of the threat landscape* not only in the abstract but also at the level of what specifics they can look for to find the attacker' (Barnum, 2014).

Furthermore, Tyler Moore has connected the informational asymmetry among organizations facing similar cyber threat vectors to their under-investment in cybersecurity: lack of risk awareness will likely result in a shortfall of resources devoted to risk mitigation (Moore, 2010; and Gordon, Loeb, and Lucyshyn, 2003).

*What is information sharing for cybersecurity?* For the purposes of this article it is defined as the exchange of information that promotes organizational and collective cybersecurity, encompassing data on cyber risks, threats, and incidents – especially hostile incidents – and the operational responses to them. IS may take place among private sector organizations, and between them and government regulators. The information shared includes *administrative and business continuity data* (threat intelligence and analysis), *technical indicators* (alerts, indicators of potentially hostile events or the behaviour of a certain hostile actor); *operative information* on practical

<sup>6</sup> Such an incident may be defined as 'an event which changes the security posture of an organization or circumvents security policies developed to prevent financial loss and/or the destruction, theft, or compromise of proprietary information. Also, an event investigated by an organization due to unusual activity, that cannot be explained as a consequence of normal operations.' (CSIRT, n/d). See also the definition of "incident" in Article 4 (7) of the NIS.



measures for mitigating hostile cyber activity through network defence (tool configurations); and *protected information* such as personal data or organizational intellectual property (Johnson et al., 2016)<sup>7</sup>. Increasingly, IS may also encompass *responsible disclosure of cyber vulnerabilities*, a topic beyond the scope of this analysis and noted in the conclusion as one of the developing challenges for IS platforms<sup>8</sup>.

Some well-known examples of cybersecurity information sharing platforms and consortia that operate on a global basis include Computer Emergency Response Teams (CERTs)<sup>9</sup>, Computer Security Incident Response Teams (CSIRTs)<sup>10</sup>, the Forum of Incident Response and Security (FIRSTs)<sup>11</sup>, the Cyber Threat Alliance, and the US-initiated Information Sharing and Analysis Centres (ISACs) and Cyber Information Sharing and Collaboration Program (CISCP)<sup>12</sup>. These and other platforms utilize a growing diversity of coordinated communications protocols to relay relevant data and indicators among participants<sup>13</sup>. Platforms and protocols may also be specified by IS regulation applicable in a particular jurisdiction: one example discussed at greater length herein is the specification of CSIRT platforms in the EU NIS Directive<sup>14</sup>. Participation of private sector organizations in specific IS platforms available in a given jurisdiction may be either required by government regulation or voluntary (Bedrijfsrevisoren, De Muynck and Portesi, 2015). Although the scope of the present analysis does not permit a full treatment of these diverse regulatory regimes (Gibbons, 1997; and Nolan,

2015)<sup>15</sup>, the two chosen for analysis herein represent these two modalities.

## 2. The Challenge of Private Sector Ambivalence

Despite the advocacy of IS by many theorists, regulators, and practitioners, some private sector organizations continue to approach it with ambivalence (Aviram and Tor, 2004). This is because exchanges that bring real value to participants require trusted interactions that reveal potential or actual organizational vulnerabilities, operational preparedness and response capabilities, and sharing of data processed by the organization. Yet where regulation does not compel IS, private sector actors may opt out of voluntary sharing<sup>16</sup>. Even when sharing is mandated by a regulator, and when government agencies contribute their own knowledge of cyber threats and risks for the benefit of all participants, private sector actors' participation may be less than optimal (Kopp, Kaffenberger and Wilson, 2017). They attribute several drawbacks to current information sharing platforms, which may be characterized as operative or normative. The *operative reasons* include challenges such as:

- *Imperfect trust relationships* among participants, who may be market competitors;
- *Lack of transparency regarding the efficiency and confidentiality of IS platforms*, including the use of shared data by any participating government agencies for non-cybersecurity purposes (Johnson et al., 2016);
- *Undue exposure of organizational vulnerabilities, preparedness and response measures*;
- *Costs related to IS* including recruitment, training, and retention of appropriate personnel; and organizational time spent on IS, including time devoted to "false positives" (Powell, 2005; Etzioni, 2014; and Gordon, Loeb, and Lucyshyn, 2003).

7 For present purposes, IS does not include first-level exchanges with military or covert state actors, although such actors may indirectly share via other government entities.

8 See, for example, CERT Guide to Coordinated Vulnerability Disclosure (2017).

9 See US-CERT. (n/d).

10 See ENISA. (2016).

11 See FIRST. (n/d).

12 See Cyber Threat Alliance. (2014).

13 Among these are the Incident Object Description Exchange Format (IODEF), Traffic Light Protocol (TLP), Structured Threat Information eXpression (STIX), Trusted Automated eXchange of Indicator Information (TAXII), Cyber Observable eXpression (CybOX) and the DHS Automated Indicator Sharing (AIS) (Van Impe, 2015, March 26; and DHS, n/d).

14 See NIS Articles 9 and 12. For cyber event taxonomies for CSIRTs, see ENISA. (2018).

15 The 2015 US Cybersecurity Information Sharing Act is one example, stipulating that one of the aims of such sharing is "...[t]o detect, prevent, or mitigate cybersecurity threats or security vulnerabilities..." (Cybersecurity Information Sharing Act, 2015).

16 The issue of market failure as it impacts cybersecurity is not within the scope of this article, although it does constitute a critical impetus for regulatory intervention for IS.



Normative challenges include:

- Exposure to legal liability with respect to protected personal data and intellectual property, either entrusted by others to the organization or developed internally; and
- Concerns of susceptibility to *antitrust claims* flowing from IS<sup>17</sup>.

Because of the present financial, disruptive, and reputational costs of hostile cyber activity for both governmental and private sector stakeholders, the stakes are high for achieving a clearer analytical understanding of how to incentivize IS for all actors. Both operative and normative drawbacks, whether actual or perceived, need to be addressed by IS platforms that are concerned with their own sustainability and effectiveness (Vazquez et al., 2012). Moreover, the challenges of the current cyber threat landscape require not only agreement on the part of organizational actors that IS strengthens cybersecurity and resiliency for all, but also the development of a high level of mutual trust among these actors (Nelson, 2017). Overall, many practitioners and regulators are seeking to improve IS mechanisms and support private sector buy-in and participation in order to better leverage IS as a critical factor for mitigating hostile activity in cyberspace (Johnson et al., 2016; and Bedrijfsrevisoren, De Mynck and Portesi, 2015, p. 6)<sup>18</sup>.

---

***Because of the present financial, disruptive, and reputational costs of hostile cyber activity for both governmental and private sector stakeholders, the stakes are high for achieving a clearer analytical understanding of how to incentivize IS for all actors.***

---

### 3. Comparing the EU NIS and the IFC3

In this second part of this article, we will review and analyse two relatively new initiatives that aim to promote

jurisdictional cybersecurity among private sector and government stakeholders through the inclusion of IS platforms as an integral, strategic element of overall preparedness, response and resilience. Comparison between the EU's NIS-mandated platform for IS and Israel's Cyber and Finance Continuity Center (FC3) requires methodological caution, as the regulation supporting each initiative differs in nature and applicability in their respective jurisdictions. Nonetheless, we propose that, as each of these nascent platforms develops a *praxis* for IS, they may mutually benefit from the experience of their counterpart. ■



---

17 For example, see a discussion of normative liability issues under the 2015 US Cyber Security Information Act see Schwartz, A. et al. (2017).

18 On IS measures in multilateral agreements and initiatives, see Housen-Couriel, D. (2017).



## REFERENCES

- Aviram, A. and Tor, A. (2004). Overcoming Impediments to Information Sharing. *55 Ala. L. Rev.* 231.
- Barnum, S. (2014). Standardizing cyber threat intelligence information with the structured threat information expression. pp. 5-6.
- Bedrijfsrevisoren, D., De Muyck, J, and Portesi, S. (2015). Cyber security information sharing: an overview of regulatory and non-regulatory approaches. *ENISA*. pp. 6-10.
- Chabrow, E. (2017, November 14). How Information Sharing Helped Curtail WannaCry Harm. *BankInfo Security*. Retrieved from: <https://www.bankinfosecurity.com/interviews/how-info-sharing-helped-curtail-wannacry-harm-in-us-i-3772>
- CSIRT. (n/d). Definition of an incident. Retrieved from: [http://www.csirt.org/incident\\_report/index.html](http://www.csirt.org/incident_report/index.html)
- Cyber Threat Alliance. (2014). A new way to share threat intelligence.
- Cybersecurity Information Sharing Act. (2015). S. 754, 114<sup>th</sup> Cong. Title I, Sec. 104.
- Deloitte and Fraunhofer. (2013). Cybersecurity: The perspective of information sharing.
- Department of Homeland Security. (2018, August 31). Cyber Information Sharing and Collaboration Program (CISCP). Retrieved from: <https://www.dhs.gov/ciscp>
- Department of Homeland Security. (n/d). Automated Indicator Sharing (AIS). Retrieved from: <https://www.dhs.gov/ais>
- ENISA. (2016). CSIRT capabilities: How to assess maturity? Guidelines for national and governmental CSIRTs.
- ENISA. (2017). Information Sharing and Analysis Centers (ISACs): Cooperative Models.
- ENISA. (2018). Reference incident classification taxonomy.
- European Commission. (2018, May 4). *State of play of transposition of the NIS Directive*. Retrieved from: <https://ec.europa.eu/digital-single-market/en/state-play-transposition-nis-directive>.
- European Commission. (2018, July 19). Commission asks Member States to transpose into national laws the EU-wide legislation on cybersecurity. Retrieved from: <https://ec.europa.eu/digital-single-market/en/news/commission-asks-member-states-transpose-national-laws-eu-wide-legislation-cybersecurity>
- Etzioni, A. (2014). The Private Sector: A Reluctant Partner in Cybersecurity. *15 Geo J. Int'l Aff.* 69.
- FIRST. (n/d). FIRST Malware Information Sharing Platform (MISP) instance. Retrieved from: <https://www.first.org/global/sigs/information-sharing/misp>
- GFCE. (2017). CERT Guide to Coordinated Vulnerability Disclosure. *Global Good Practices: Coordinated Vulnerability Disclosure*.
- Gibbs, M. R., Shanks, G. and Lederman. R. (2005). Data Quality, Database Fragmentation and Information Privacy. *Surveillance and Soc.* 45
- Gibbons, L. J. (1997). Regulation, Government Regulation, or Self-Regulation: Social Enforcement or Social Contracting for Governance in Cyberspace. *6 Cornell J.L. & Pub. Policy.* 475.
- Gordon, L., Loeb, M. and Lucyshyn, W. (2003). Sharing Information on Computer Systems Security: An Economic Analysis. *22 J. Acct. & Pub. Policy.* pp. 461-485.
- Hartman, B. et al. (2012). Breaking Down Barriers to Collaboration in the Fight Against Advanced Threats. RSA Security Brief. Retrieved from: <https://www.emc.com/collateral/industry-overview/11652-h9084-aptbdb-brf-0212-online.pdf>
- Housen-Couriel, D. (2017). An Analytical Review and Comparison of Operative Measures Included in Cyber Diplomatic Initiatives. *GCSC Issue Brief 1.* pp 46-84.
- Johnson, C., et al. (2016). NIST Guide to Cyber Information Threat Sharing. *Special Publication.* 800-150.
- Kopp, E., Kaffenberger, L. and Wilson, C. (2017). Cyber Risk, Market Failures, and Financial Stability. pp 6-8.
- Ministry of Finance. (2017, September 4). *Finance Cyber and Continuity Centre (FC3)*. Retrieved from: <https://docs.google.com/viewer?url=http%3A%2F%2Fwww.export.gov.il%2Ffiles%2Fcyber%2FFC3.PDF%3Fredirect%3Dno>

Moore, T. (2010). The Economics of Cybersecurity: Principles and Policy Options. *3 Int. J. Crit. Infrastructure Prot.* 103. p. 8.

Nelson, B. (2017). The Value of Information Sharing. *The Clearing House*. Retrieved from: <https://www.theclearinghouse.org/research/banking-perspectives/2017/2017-q2-banking-perspectives/the-value-of-information-sharing>.

Nolan, A. (2015). Cybersecurity and Information Sharing: Legal challenges and Solutions. *Cong. Research Serv.*, R43941.

Powell, B. (2005). Is Cybersecurity a Public Good? Evidence from the Financial Services Industry. *1. J. L. Econ. & Policy.* 497. p. 507.

R. Gibbs, M., Shanks, G., & Lederman, R. (2005). Data Quality, Database Fragmentation and Information Privacy, *3 Surveillance & Soc.*

Richet, J-L. Market Failure Mechanisms in Cybersecurity. *WISP Proceedings 2012.* p 26.

Schwartz, A. et al. (2017). Automatic Threat Sharing: How Companies Can Best Ensure Liability Protection When Sharing Cyber Threat Information with Other Companies or Organizations. *50 U. Mich. J. L. Reform* 887.

US-CERT. (n/d). Information Sharing Specifications for Cybersecurity. Retrieved from: <https://www.us-cert.gov/Information-Sharing-Specifications-Cybersecurity>.

Van Impe, K. (2015, March 26). How STIX, TAXII and CyBox Can Help with Standardizing Threat Information. *Security Intelligence*.

Vazquez, D. et al. (2012). Conceptual Framework for Cyber Defense Information Sharing within Trust Relationships. *4<sup>th</sup> International Conference on Cyber Conflict, CCDCOE*. [eds. C. Czossek, R. Ottis, K. Ziolkowski].

WannaCry Ransomware Attack and International Information Sharing. (n/d). Retrieved from : <https://www.billingtoncybersecurity.com/wannacry-ransomware-attack-international-information-sharing/>.

World Economic Forum. (2018). *Global Risk Report*.

Zheng, E. and Lewis, J. A. (2015). Cyber Threat Information Sharing: Recommendations for Congress and the Administration. Center for Strategic and International Studies.



OPINION

## CAN A PUBLIC TENDER BE A THREAT TO IT INFRASTRUCTURES IN PUBLIC INSTITUTIONS?



**PAWEŁ SAWICKI**

is an expert in criminal cases involving IP rights and cybersecurity and has extensive experience in the prosecution of cybercrime. He has been appointed as anti-piracy counsel for the world's leading software producers (Microsoft, Autodesk and Adobe) and leads the criminal enforcement programme for BSA | The Software Alliance in Poland. He has represented clients from IT software and chemicals sectors before the authorities and courts in connection with violations of intellectual and industrial property rights; he has also assisted many clients in relation to internal investigations.

Paweł is a member of the Association of Certified Fraud Examiners (ACFE).

First, let your imagination run free.

Let's imagine that an intelligence agency of a foreign country wants to access personal computers of all Polish deputies and senators. And I do not mean the physical seizing of their computers, but undetected ongoing access to everything what is done on them. It would make it possible to trace the planning process for the legislative acts before they even go public or imperceptibly change a few words in them, why not? It would make it possible to get access to private conversations about what exactly the opposing parties think about the governing party and vice versa. It would enable them to search for proof of unethical behaviour or provoke one, or even place compromising materials and incite an international scandal. With unfettered access to somebody's computer, the only limitation is our imagination. Tempting? Unreal?

Mission impossible? Because no one can install spyware on a deputy's computer, right?

If not the computers of the deputies and senators, then maybe somebody would be interested in hacking the database of the Polish Social Insurance Institution (ZUS) and stealing personal information of millions of Poles? How much would the data be worth on the black market? Let's try to assess that. On the Internet, the price for a regular database starts from PLN 0.10 for a record. The data available in ZUS are inevitably more valuable and thus worth at least PLN 1.00 for a record. It can be easily assessed that even a small data leakage – let's say of 2 million records – would be worth around several tens of millions Polish zloty on the black market, not to mention that such a database could be sold more than once.

In August 2016, there was an incident described initially as 'a leakage from the PESEL database'. PESEL means Universal Electronic System for Registration of the Population; it is a massive central database, currently managed by the minister in charge of computerisation. This register stores identities of all Polish citizens and foreigners residing in Poland. They are extremely sensitive and therefore access to the data is very restricted. The PESEL system is mainly used by the authorities responsible for the safety of the country: the police, the Internal Security Agency, the Central Anti-corruption Bureau, the Public Prosecutor's Offices, courts, but also tax offices and bailiffs. The latter were initially to be blame for the 'data leakage'. On 12 August 2016, the Ministry of Digital Affairs informed the law enforcement agencies about an extremely atypical behaviour of the entities which collect data from the PESEL database. In a relatively short period of time, at night, the ministry's servers received hundreds of thousands of requests, and data of more than 1.4 million people were downloaded. At first, it might have looked like a cyberattack. However, after the investigation by the Public Prosecutor's Office in Warsaw, it turned out that it was not a cyberattack, but an uncommon hyperactivity of bailiffs' offices. It seems that the data did not fall into unauthorised hands after all.

However, the case re-emerged after two years. In July 2018, the public learned that a private company GetBack S.A., until a recent big financial scandal one of the most rapidly growing entities in the debt collection sector, also had access to the PESEL database. The company had issued bonds for the total value of PLN 2.5 billion and was unable to redeem them. The management of the company was temporarily arrested. In 2015, the Ministry of Internal Affairs, which was responsible for managing the PESEL database at that time, set the precedent by granting consent to Kancelaria Prawna GetBack, which was related to GetBack S.A., to share address details from the PESEL register by using data telecommunication devices through verification. It was the first time in history when a private debt collection company had gained access to this database. Clearly, a completely unreliable entity was given an unusually high level of trust. In this situation, the question that arises is: who verifies the credibility and reliability of the entities that are given such extensive rights?

This example shows very clearly how valuable the data are of which public institutions keep custody of.

---

***Databases collected by public institutions contain unique information about each of us and therefore there are many people who would like to acquire it.***

---

The public sector in Poland includes a huge number of institutions, public offices and therefore – computers. It is enough to point out that every fifth Pole works in the public sector. Public administration, offices, uniformed services, health care institutions, and cultural institutions constitute thousands of entities, each of which uses IT technology. Regardless of whether it is a small school or the National Bank of Poland, they all create and collect massive amounts of data. Databases collected by public institutions contain unique information about each of us and therefore there are many people who would like to acquire it.

The public sector is one of the major investors when it comes to IT. Public institutions spend a considerable amount of public funds on technology and their expenses continue to rise. For instance, the public tenders for the supply of IT services announced and won in 2016 amount to PLN 4 billion. The amount increased to PLN 5.1 billion in 2017. New investments are driven by the EU funds, and the purchases are made by small offices as well as big ministries with thousands of computers in their infrastructure. Computerisation is required because of the changes in legislation, such as the GDPR which sets high standards regarding personal data protection safeguards and demands improvements in IT security.

Despite growing investments, the public sector is identified as the most threatened by cyberattacks. It seems obvious, taking into account the fact it has the information cybercriminals are looking for. In August 2014, a DDoS attack paralysed the websites of the Chancellery of the President and the Warsaw Stock Exchange. In November 2014, the IT systems of the Polish National Electoral Commission were attacked and as a result employee data were stolen. In February 2017, the website of the Polish Financial Supervision Authority was blocked, presumably by North Korean hackers whose aim was to target the



whole banking sector in Poland. Finally, in June 2018, numerous governmental IT systems, including CEPIK (Central Register of Vehicles and Drivers) or ePUAP (Electronic Platform of Public Administration Services) stopped working, most likely as a consequence of multiple DDoS attacks.

These are just a few examples of successful attacks. The ones that failed have never gained public attention. If we consider that each day in Poland there are 100,000 attempts of cyberattacks, we can be sure that sooner or later we will witness at least one successful and spectacular attack on an unprecedented scale.

Let's go back to the 'fantasy scenario'. Suppose that someone would like to keep track of cyber activity of Polish parliamentarians and have access to their IT resources. How can one accomplish that? To begin with, such a person should start a limited liability company (Sp. z o. o.) selling computers and other IT equipment and software. Then, the company should participate in a public tender for the supply of computers and software announced by the Sejm Chancellery. It should not be a problem to win the bidding since in the Polish reality of public tenders it would be sufficient to offer the lowest price. Next step would be to buy computers from a computer hardware reseller and install spyware with a cleverly disguised computer virus.

The last thing would be to deliver the computers to the contractor and wait until they connect to the IT infrastructure of the Sejm. It seems to be very easy but also extremely unreal. After all, the plan could never be successful because the attempt would undoubtedly be detected by the respective services. It appears, however, that it is not necessarily correct.

In April 2016, under the public service contract, the Sejm Chancellery received 15 personal computers with office software. The hardware was collected and was ready to be handed over for use. Unfortunately, it turned out that there was a problem activating office programs – the activation keys delivered by the supplier did not work and therefore the installation process and activation of the office programs could not be completed. Apart from that, everything seemed to be in order. The computers operated perfectly, the operating system worked as it should. The employees of the Sejm Chancellery asked the software manufacturer for support in establishing the sources of the problem with activation. It turned out that the provided keys were blocked because they had been abused – the keys had been previously used multiple times. Further explanatory proceedings led to the finding that illegal copies of a popular computer system had been installed on the delivered computers with affixed counterfeit certificates of authenticity.

***If we consider that each day in Poland there are 100,000 attempts of cyberattacks, we can be sure that sooner or later we will witness at least one successful and spectacular attack on an unprecedented scale.***



The fraud scheme was very simple: a small company, without a physical office, infrastructure, a warehouse or employees, was buying PCs of well-known brands. The computers either had already been equipped by the manufacturer with a free operating system or did not have an operating system at all. The ordering party demanded computers with a leading commercial operating system that required a fee-based license. The company which won the tender installed the commercial operating system on its own. In order to increase its credibility and make the illicit activity appear legal, the company affixed counterfeit labels imitating the certificates of authenticity purporting to originate from the leading manufacturer of the computer programs. The computers operated properly; however, the operating system on the equipment was unauthorised. In that way, the company could save approx. PLN 400 – 500 on one computer. It was sufficient to be competitive.

At some point, the scale of the phenomenon increased to the extent that the same companies – previously not recognised in the market – started winning the majority of the tenders. These companies began eliminating companies which had been associated with the IT services for the public sector for many years. In some cases, these well-known companies also started to look for ‘alternative’ solutions to lower the costs of the offered equipment.

Therefore, since it was possible to install a ‘pirated copy’ of the software and deliver such computers to a public institution, what could preclude someone from installing on computers other ‘extra’ programs with various specifications?

The Sejm Chancellery organised a tender, chose an offer, collected their order and used computers with illegal copies of the operating system. Imagine the consequences the incident would have had if the computers had been integrated into an internal infrastructure of an institution and had had additionally installed spyware or other custom-written viruses?

The moment the fraud was revealed (let me remind you that it could have not been discovered at all if the activation keys to other programs had worked or the ordering party had requested computers with the operating system only), the investigation proceedings

conducted by the police and the Public Prosecutor’s Office were initiated. It turned out that the scale of this type of offences is enormous, with dozens of public institutions becoming unaware victims of fraudulent suppliers of IT products.

It is worth noting that the first revealed and defeated attempt to deliver personal computers with illegal copies of the operating system took place in a big tender organised by... the Polish Police Headquarters in 2015. Obviously, it was not the first tender in which the fraudulent practice had occurred; however, it was the first time when the law enforcement agencies had realised its extent. The fact that unfair tenderers decided to supply the police with illegal software demonstrates their certainty of their impunity. Thus, the conclusion is they must have successfully conducted similar deliveries in the past. In this case, this happens to be true.

---

***It turned out that the scale of this type of offences is enormous, with dozens of public institutions becoming unaware victims of fraudulent suppliers of IT products.***

---

In November 2015, after disclosing a number of attempts (failed and successful) to deliver computers with illegal copies to several ministries, the Public Procurement Office published on its website a letter to the President of Lewiatan – the Polish Confederation of Private Employers in the Digital Technology Industry (Polski Związek Pracodawców Technologii Cyfrowych Lewiatan) regarding the identified risks related to offering unlicensed software in public procurement procedures. The letter pointed out for the first time the scale of the problem and drew attention to the way the perpetrators act and how to avoid similar events.<sup>1</sup>

However, back then, the problem failed to raise any greater awareness.

On 13 January, 2017, the Ministry of Family, Labour and Social Policy published an official statement on its

---

<sup>1</sup> The text of the letter was published on the website: [https://www.uzp.gov.pl/\\_data/assets/pdf\\_file/0007/31012/Nielegalne\\_oprogramowanie\\_w\\_zamowieniach\\_publicznych.pdf](https://www.uzp.gov.pl/_data/assets/pdf_file/0007/31012/Nielegalne_oprogramowanie_w_zamowieniach_publicznych.pdf)

website as a response to the then current press reports. The statement confirmed that in May 2015, the Ministry of Labour and Social Policy purchased computers with illegal software. The computers were purchased by the office to carry out tasks arising from the Act on the Big Family Card. The number of computers was 2,500 and the value of the tender was estimated at PLN 10.5 million. The computers were delivered to the municipalities throughout the country.

In March 2018, the Central Anti-Corruption Bureau informed about the arrests of owners of the companies that participated in tenders for the supply of IT equipment and delivered computers with 'pirated' software. At that time, the law enforcement agencies had evidence which confirmed that unlicensed software was found on 3,256 computer units worth PLN 9.5 million that had been delivered to public institutions throughout the country. Among the affected institutions were the Sejm Chancellery, the Office of the Marshal of Warmińsko-Mazurskie Voivodeship in Olsztyn, the City Halls of Poznań, Radom, Kraków and Tychy, and a university. This fraud scheme took place between 2012 and 2016.

What is the real scale of the problem? Nobody knows. The law enforcement agencies are tracking the sources and find computers which were bought by public institutions years ago and which have functioned within the infrastructure of a given institution until now. Many entities are surprised when they discover anomalies; in their view, if everything is in order because, i.e. their computers work as they should and there are no problems with the equipment or software functionality, they do not have reasons to think otherwise. On the other hand, it sometimes happens that an institution discovers anomalies years after the purchase. They usually find out something is wrong when they need to reinstall the software and use the activation key again. It turns out that the activation is not successful because the key was blocked due to a multiple abuse of the key by other users who received exactly the same activation key.

It is a well-known fact that public tenders are exposed to great risk, both actual and legal. The problems arise already at the stage of preparing the specifications and the terms and conditions of the tender where potential modifications of the conditions with regard to the service may affect the result

of the tender, i.e. the selection of the tenderer. It is potentially a fertile ground for any corrupt activities.

The fact that persons who perform public procurement proceedings lack specialisation constitutes another problem. It often happens that within one institution there is only one person who is responsible for the purchase of cleaning products and IT technology. It is impossible to possess expert knowledge in every field. Obviously, the persons are supported by individual departments for which the purchase is made. However, in some situations, it is not sufficient. No officials in a small municipality can be blamed for not having sufficient expertise in recognising counterfeit certificate of authenticity for a computer program.

And finally, we come to the most important issue. Since the price is practically the only criterion that determines who wins the bid, it is very common that the awarding process is done at the expense of the quality of products or services. It can be seen in almost every sector: from stationery supplies to construction works.

---

***Since the price is practically the only criterion that determines who wins the bid, it is very common that the awarding process is done at the expense of the quality of products or services.***

---

In some of the above-mentioned tenders for the supply of computers with software, as a result of which unauthorised copies of software were delivered, there were only two criteria that were taken into account when selecting the offer: the price and the warranty period. The price has always represented over 90% of the total points in the offer evaluation criteria. In practice, the company which gives the lowest price usually wins the tender. Neither the quality of the equipment nor the credibility of the supplier is significant. In those particular tenders, the ordering party did not verify or assess the tenderers. It was of no significance whether the supplier enjoyed a good reputation and had a track record as a supplier in the IT market or, by contrast, was a rather unknown company with a minimum share capital and a virtual office. As a consequence, the equipment delivered to the institutions did not only have unauthorised software installed (which constituted a risk in itself) and it was either defective and of poor quality, or previously used and refurbished.



Over the last few years, Polish public institutions have been unaware of the use of unauthorised computer programs. The operating systems installed on their computers came from unknown sources. They were not supplied by computer manufacturers themselves. This fact alone puts their IT infrastructures at risk of using malware against them. Unfortunately, the applicable laws and standard practice have shown that it is not difficult to introduce malicious programs which often become part of the network infrastructure of the entities responsible for electronic data that is critical for the security of the country and its citizens.

It seems necessary to stop concentrating on the price as the decisive criterion in awarding a public contract. It is important to educate people responsible for organising tenders for IT equipment in cybersecurity and to supervise the key procurement proceedings of the competent authorities of the country – not only in the context of anti-corruption policies. There should be effective methods of verifying potential suppliers early on, starting from the assessment of an offer. Computer equipment and software should come from reliable sources. It is also worth considering closer cooperation between the ordering parties and the computer and software manufacturers on new technological solutions, also in terms of the analysis of authenticity and originality of IT products and verification of their sources. ■



ENTREPRENEURIAL SUCCESS STORY

## PROTECTING TODAY AGAINST THE THREATS OF TOMORROW



### LOTHAR RENNER

Lothar Renner leads Cisco's Security business in Northern Europe, Eastern Europe, Russia/CIS and Switzerland. He is responsible for creating and delivering the security strategy and driving sales growth. He oversees more than 30 countries with an emphasis on keeping customers secure in an increasing threat landscape.

Lothar and his team engage with hundreds of leaders in the enterprise, public sector, service provider and partner led markets, enabling them to transform organisations with innovative technologies from Cisco.

Prior to leading Cybersecurity, Lothar led the Services business for Central Europe. Lothar joined Cisco 20 years ago in Germany. He has held numerous leadership positions in Cisco in Germany and Central Europe.

**The digital world is expanding at an unprecedented rate, and attack opportunities are expanding just as quickly. Attackers have unlimited attempts and resources to be effective, while defenders have to win each and every time. To combat threats, security needs to go beyond tracking and detection and push the boundaries of today's security technologies to work against tomorrow's exploits. This is where Talos – Cisco's Threat Intelligence Organization – takes the initiative by providing the most comprehensive security and threat intelligence solutions in the industry.**

The Cisco Security ecosystem covers email, networks, cloud, web, endpoints, and everything in between. With the sheer size and breadth of Cisco Security's portfolio and the incoming telemetry from Cisco's customers and products, Cisco has more visibility than any other security vendor in the world. This unique visibility delivers greater context from many data points during an incident or campaign. Along with other resources such as open-source communities and internal vulnerability discovery, Talos is able to move faster and create more comprehensive assessments of ongoing threats.

### Breadth and depth

Protecting the network requires both breadth and depth of coverage. While some research teams limit their focus to a few areas, Talos is dedicated to helping provide protection against an extensive range of threats. Talos' threat intelligence supports a wide range of security solutions including Next-Generation Intrusion Prevention System (NGIPS), Next-Generation Firewall (NGFW), Advanced Malware Protection (AMP), Email Security Appliance (ESA), Cloud Email Security (CES), Cloud Web

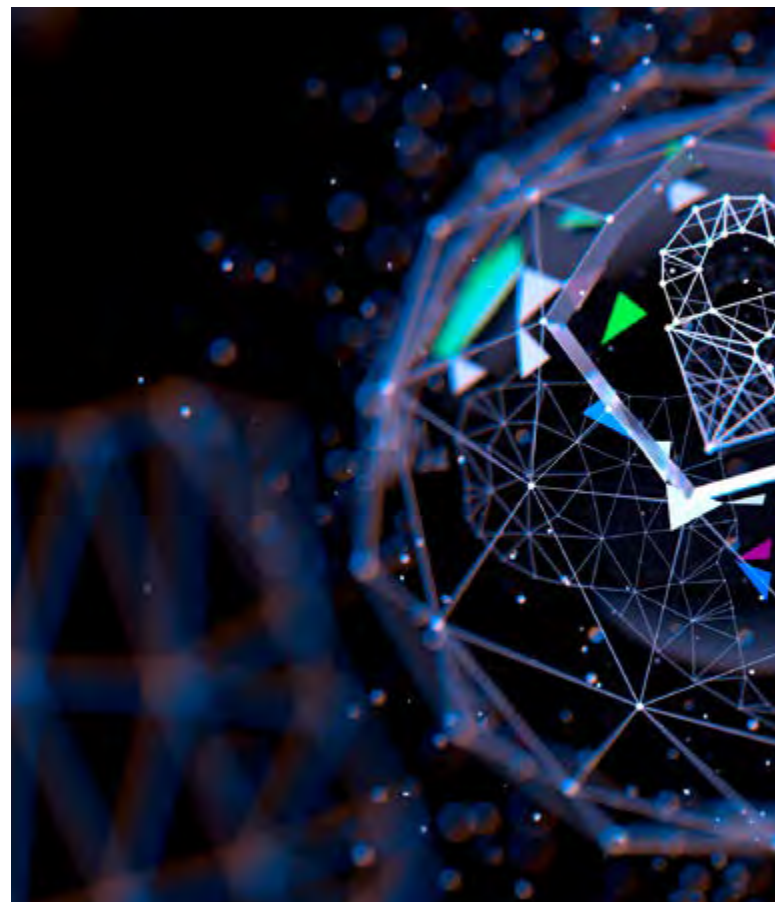
Security (CWS), Web Security Appliance (WSA), Umbrella, and ThreatGrid, as well as numerous open-source and other commercial threat protection systems. These products directly contribute to Talos' telemetry, which in turn is utilized to provide detection content that can be deployed in any environment to protect all types of assets:

- **Email security.** Each day, Talos inspects more than 300 billion emails, drawing on layering detection technologies, like outbreak filters and machine learning-based reputation filters, along with Cisco's Advanced Malware Protection (AMP). With all of the features combined, Talos blocks approximately 200 billion malicious emails a day, which equates to approximately 2.3 million blocks per second.
- **Web visibility.** Cisco Web Security technologies have a reputation for detecting and identifying new and emerging web exploitation techniques. Talos has insight into nearly 17 billion web requests each day, drawing on multiple protection methods, including our AMP technology to protect our users.
- **Vulnerability-based protection.** Talos is well-known in the industry for its excellence in detecting vulnerabilities, exploits, and malware that emerge daily. Using high-quality, rapid releases, we keep our customers up to date with vulnerability-based protections from the latest threats. Talos has proven this time and again in third-party validation with NSS Labs Inc., a leading independent security research agency. We have come first in the Network NGIPS and NGFW tests in detection rate for the past seven years.
- **Advanced Malware Protection.** Protecting against the onslaught of malware requires innovative and advanced detection technologies, massive amounts of intelligence gathering, reverse engineering, and analytics. Talos utilizes all of this to develop malware protections, post-compromise protection, reputation services and analysis tools to locate threats as they appear "in the wild". These capabilities are included in all Cisco products for protecting hosts, mail gateways, and network assets – truly protecting customers before, during, and after the threat.

### Comprehensive and Actionable Threat Intelligence

The core component of any holistic security strategy is solid, actionable intelligence. Talos has built one of the most comprehensive intelligence gathering and analysis platforms in the industry. Through the ClamAV®, SNORT®, Immunit®, SpamCop®, Talos Reputation Center, Threat Grid®, and other Talos user communities we receive valuable intelligence that no other security research team can match. Through collaboration with users and customers around the globe utilizing our Crete program, Talos is able to detect regionalized threats as they emerge.

Talos also collects more than 1.1 million malicious software samples a day by compiling data acquired from product telemetry along with honeypots, sandboxes, and industry partnerships in the malware community. Its advanced analysis infrastructure automatically analyses samples and rapidly generates detection content to mitigate threats on a daily basis. This provides meaningful insight into the threat landscape and an unparalleled perspective as adversaries attempt to compromise users.



Whether identifying new malware families targeting point-of-sale terminals, widespread malvertising networks, or even threats that pose a risk to core services on the internet, Talos can be counted on to identify, research, and document adversaries. During every investigation, it identifies multiple ways customers can defend against threats. Cisco customers benefit by having this threat intelligence research and protection built into every Cisco Security product. Additionally, Talos shares this information with the public via blogs, Snort rules, conferences, and white papers to help create a safer internet for all and help introduce obstacles for adversaries.

### **VPNFilter – Cisco Talos reveals a 500,000-strong botnet**

In one of my previous European Cybersecurity Journal articles I described how Cisco Talos actively investigated “Nyetya”, one of 2017 most destructive ransomware campaigns. Talos’ initial analysis pointed to the attack starting in Ukraine from software update systems for a Ukrainian tax accounting package called MeDoc. Later, MeDoc itself confirmed those suspicions. The attack was

targeting companies doing business in and with Ukraine. The intel from Talos saved our customers and the general public precious hours of searching for phantom email and maldocs that did not exist (Chiu, 2017, June 27).

This year Talos also made the headlines with its discovery. For several months, Talos has been working with public and private-sector threat intelligence partners and law enforcement in researching an advanced, likely state-sponsored or state-affiliated actor’s widespread use of a sophisticated modular malware system called VPNFilter. In particular, the code of this malware overlapped with versions of the BlackEnergy malware – which was responsible for multiple large-scale attacks that targeted devices in Ukraine. While this wasn’t definitive by any means, Talos have also observed VPNFilter, a potentially destructive malware, actively infecting Ukrainian hosts at an alarming rate, utilizing a command and control (C2) infrastructure dedicated to that country.

Both the scale and the capability of this operation were concerning. Working with partners, Talos estimated the number of infected devices to be at least 500,000 in at least 54 countries. The known devices affected by VPNFilter were Linksys, MikroTik, NETGEAR and TP-Link networking equipment in the small and home office (SOHO) space, as well as QNAP network-attached storage (NAS) devices. The behaviour of this malware on networking equipment was particularly concerning, as components of the VPNFilter malware allowed for theft of website credentials and monitoring of Modbus SCADA protocols. Lastly, the malware had a destructive capability that could render an infected device unusable, which had the potential of cutting off internet access for hundreds of thousands of victims worldwide.

The ultimate goal of this attack was likely to leverage infected devices for a much larger scale attack, but individual devices were also at risk of data theft. The attackers included a kill switch that could make all of the infected devices inoperable – covering their tracks and eliminating internet access for hundreds of thousands. They also created its own private TOR network (an anonymous network of devices) that could share data and enable them to carry out a coordinated mass attack (Largent, 2018, May 23).





### Innovative Detection Technologies

The examples above show that it is one thing to respond to new threats, and it is another to protect against emerging and new ones. Talos is constantly searching for new vulnerabilities and threats that could affect our customers. When new vulnerabilities are discovered, Talos releases coverage to protect against these zero-day threats while the affected vendors develop and test their patches. This means that Cisco customers can control the threat while waiting for patches from their vendors using Talos' zero-day vulnerability protections.

Talos is also actively engaged in locating new malicious websites, botnet, command and control servers, and other malicious sites on the internet. Once located, this information is catalogued and consolidated into comprehensive IP blacklists and URL-altering feeds, which are distributed to our customers as well as shared with industry partners in order to make the internet a safer place.

For Cisco customers, Talos' skills and research translate directly into award-winning products and services. Even if you're not a Talos customer, you reap the benefits from Talos' research efforts that are provided to the community. Talos provides a uniquely comprehensive and proactive approach to protecting your network with a history of leadership and success in the security industry.

### Holistic approach

Cisco's strategy combines "best of breed" portfolio with an architectural approach to security, making it simple, open, and automated. This means products are integrated and share context and threat information, so that if you see a threat once, you can stop it everywhere. We understand that in order to be effective, security needs to be built into the network, and not just added on. The network is the only place that brings together all the elements for a secure digital future.

The choice is simple. Cisco offers a comprehensive set of security solutions, from the endpoint to the network to the cloud, powered by real-time threat intelligence from Talos. As a result, Cisco's integrated security

architecture helps organizations improve security efficiency by minimizing the time to detect threats and resolve incidents, drive both capex and opex savings, and improve both IT and security productivity. This approach pays off and is appreciated by our customers and peers, making Cisco the number one security vendor in the world (Harvey, 2018, August 22). ■

## REFERENCES

---

- Chiu, A. (2017, June 27). New ransomware variant "Nyetya" compromises systems worldwide. Retrieved from <https://blog.talosintelligence.com/2017/06/worldwide-ransomware-variant.html>
- Harvey, C. (2018, August 22). Top cybersecurity companies of 2018. Retrieved from: <https://www.esecurityplanet.com/products/top-cybersecurity-companies-2018.html>
- Largent, W. (2018, May 23). New VPNFilter malware targets at least 500K networking devices worldwide. Retrieved from <https://blog.talosintelligence.com/2018/05/VPNFilter.html>



# Cyber Threat Report CEE<sup>2018</sup>



Download our report  
and find out more:  
<http://report.cybersechub.eu>

CYBER SEC HUB



# INDUSTRY'S INITIATIVE TO INCREASE RESILIENCE OF CYBERSPACE: THE CYBERSECURITY TECH ACCORD

The Cybersecurity Tech Accord is a public commitment among more than 40 global companies to protect and empower civilians online and to improve the security, stability and resilience of cyberspace.

## OBJECTIVE

Signatories are committed to advancing the mission of the Cybersecurity Tech Accord by partnering on initiatives that improve the security, stability and resilience of cyberspace. By combining the resources and expertise of the global technology industry, the Cybersecurity Tech Accord creates a starting point for dialogue, discovery and decisive action.

Through a shared commitment and collective action, signatories aim to more effectively:

- Provide their customers, users and the developer ecosystem with information and tools that enable them to understand current and future threats and better protect themselves.
- Protect their customers and users everywhere by designing, developing and delivering products and services that prioritize security, privacy, integrity and reliability, and in turn reduce the likelihood, frequency, exploitability and severity of vulnerabilities.
- 

- Work with each other and likeminded groups to enhance cybersecurity best practices, such as improving technical collaboration, coordinated vulnerability disclosure and threat sharing, as well as ensuring flexible responses for the wider global technology ecosystem.
- Oppose efforts to attack citizens and enterprises by protecting against exploitation of technology products and services during their development, design, distribution and use.

## VALUES

Signatories of the Cybersecurity Tech Accord are united by common values as reflected in four core principles:

- Strong defense: We believe everyone deserves equal protection online irrespective of technical acumen, culture, location or motive for any malicious attack.
- No offense: We are committed to not knowingly undermining the security of the online environment, and to protecting against efforts to tamper with our products and services.

- Capacity building: We see cybersecurity as a shared responsibility and work to improve both the ability of everyone to act securely and safely online and the diversity of the security practitioner community.
- Collective response: We believe we can achieve more together and will partner within the group and more broadly to address critical cybersecurity challenges.

## COMMITMENT

*The online world has become a cornerstone of global society, important to virtually every aspect of our public infrastructure and private lives. As we look to the future, new online technologies will do even more to help address important societal challenges, from improving education and healthcare to advancing agriculture, business growth, job creation, and addressing environmental sustainability. Recent events, however, have put online security at risk. Malicious actors, with motives ranging from criminal to geopolitical, have inflicted economic harm, put human lives at risk, and undermined the trust that is essential to an open, free, and secure internet. Attacks on the availability, confidentiality, and integrity of data, products, services, and networks have demonstrated the need for constant vigilance, collective action, and a renewed commitment to cybersecurity.*

*Protecting our online environment is in everyone's interest. Therefore we – as enterprises that create and operate online technologies – promise to defend and advance its benefits for society. Moreover, we commit to act responsibly, to protect and empower our users and customers, and thereby to improve the security, stability, and resilience of cyberspace.*

*To this end, we are adopting this Accord and the principles below:*

### 1. WE WILL PROTECT ALL OF OUR USERS AND CUSTOMERS EVERYWHERE.

- We will strive to protect all our users and customers from cyberattacks – whether an individual, organization or government – irrespective of their technical acumen, culture or location, or the motives of the attacker, whether criminal or geopolitical.

- We will design, develop, and deliver products and services that prioritize security, privacy, integrity and reliability, and in turn reduce the likelihood, frequency, exploitability, and severity of vulnerabilities.

### 2. WE WILL OPPOSE CYBERATTACKS ON INNOCENT CITIZENS AND ENTERPRISES FROM ANYWHERE.

- We will protect against tampering with and exploitation of technology products and services during their development, design, distribution and use.
- We will not help governments launch cyberattacks against innocent citizens and enterprises from anywhere.

### 3. WE WILL HELP EMPOWER USERS, CUSTOMERS AND DEVELOPERS TO STRENGTHEN CYBERSECURITY PROTECTION.

- We will provide our users, customers and the wider developer ecosystem with information and tools that enable them to understand current and future threats and protect themselves against them.
- We will support civil society, governments and international organizations in their efforts to advance security in cyberspace and to build cybersecurity capacity in developed and emerging economies alike.

### 4. WE WILL PARTNER WITH EACH OTHER AND WITH LIKEMINDED GROUPS TO ENHANCE CYBERSECURITY.

- We will work with each other and will establish formal and informal partnerships with industry, civil society, and security researchers, across proprietary and open source technologies to improve technical collaboration, coordinated vulnerability disclosure, and threat sharing, as well as to minimize the levels of malicious code being introduced into cyberspace.
- We will encourage global information sharing and civilian efforts to identify, prevent, detect, respond to, and recover from cyberattacks and ensure flexible responses to security of the wider global technology ecosystem.

*To ensure a meaningful partnership is established through the implementation of the Tech Accord, we, the undersigned companies, will continue to define collaborative activities we will undertake to further this Accord. We will also report publicly on our progress in achieving these goals.*



## SIGNATORIES

ABB | ARM | ATlassian | AVAST | BITDEFENDER |  
BT | CA TECHNOLOGIES | CARBON BLACK | CISCO  
| CLOUDFLARE | CYBER ADAPT | DATASTAX | DELL |  
DOCUSIGN | ESET | FACEBOOK | FASTLY | FIREEYE |  
F-SECURE | GIGAMON | GITHUB | GITLAB | GUARDTIME  
| HP INC | HPE | INTUIT | JUNIPER NETWORKS |  
KOOLSPAN | KPN | LINKEDIN | MEDIAPRO | MICROSOFT  
| NIELSEN | NOKIA | ORACLE | RSA | SALESFORCE | SAP  
| STRIPE | TELEFONICA | TENABLE | TRENDMICRO |  
VMWARE | WISEKEY

**How, in your opinion, The Cybersecurity Tech Accord can be a step forward in boosting the security of cyberspace? Is the role of private sector as major digital services provider increasing in this process?**

Thanks to the fact that the internet-based technologies are present in every aspect of our lives, it became a key factor to protect our information systems as well as their users' privacy. As IT security professionals, our colleagues are working hard day-to-day to develop technologies which make the cyberspace a more secure territory. Nevertheless, this is a constant challenge as long as the service providers in the digital scene do not comply with certain standards, methodologies, and guidelines which they have developed together with a focus on the fundamentals of cybersecurity.

The Cybersecurity Tech Accord initiative is giving an answer to this exact challenge with providing a chance and a platform for the globally present technology companies to discuss and work towards a better protection of cyberspace and its users.

This cooperation between global players in the private sector could offer a breakthrough in the field of cybersecurity, which could not be replaced by any legislative requirement or recommendation.

– Sándor Cseledi, CEO of Balasys

**What is the added value for you, as a company, of being one of the signatories to The Cybersecurity Tech Accord?**

In Safetica, the main substance of what we do is protecting organisations and their employees against the risks of modern cyberspace. We believe that every user and every company, no matter its size or industry, deserves the right to protect their data. We perceive the added value of being committed to the Cybersecurity Tech Accord for us as a company in the cooperation with like-minded organisations to contribute to our common goal. Even though we might be competitors in business, we all share the same goal – to protect users and consumers.

– Petr Žikeš, CEO of Safetica Technologies



**In The Cybersecurity Tech Accord statement you perceive cybersecurity as a shared responsibility. What should the cooperation between different entities (namely different sectors) and stakeholders look like?**

Cybersecurity is perceived as a shared responsibility by many organisations and governments that fight directly or indirectly with digital crime. We are entering an era where every device is connected and online. As such we are becoming even more vulnerable to cyber-attacks which, nowadays, could even have life-threatening impact. No single organisation or entity can successfully defend itself against cybercrime due to the scale and complexity of modern systems and involved stakeholders. Cybersecurity could be perceived as a long chain which is as strong as its weakest link. Each link is an entity or stakeholder involved in the process. Typically, the shorter the chain, the better security it provides, but it also has less functionality.

The different entities and stakeholders having cybersecurity responsibility could be split into the following categories:

- consumer (end user/employee)
- software manufacturer
- hardware manufacturer
- researcher (or ethical hacker)
- government
- distributor
- service/product implementer
- operations/support

Each of these entities should cooperate with one another to establish good defence against cybercrime. Some types of collaboration are difficult to achieve due to intellectual property and copyrights as components are black boxes to third parties. This is where researchers can provide invaluable input about discovered vulnerabilities to manufacturers, implementers, and operations teams. Consumers on the other hand are a preferred target for attackers as they are an easy entry point to the company that can provide potential elevation of privileges and damage spread within the organisation. Consumers need to be educated by support teams and system implementers in applying good cybersecurity hygiene.

Because of the immersive growth of service providers, there is a need for growth in responsibility too. Service providers have become trusted entities and customers entrust their business and data with them. This results in a bigger responsibility and accountability of protecting customers' businesses from cyber-attacks. Therefore, service providers can significantly improve the overall state of cybersecurity through signal exchange programs aimed at recognising and eliminating threats to their services and customers quickly. Here cooperation between various providers, researchers, and governments is a key to success. The role of governments is also to recognize the need for cybersecurity via security and compliance regulations that require the use of current security standards and practices.

– Grzegorz Chuchra, CEO of Predica



# THE 3 SEAS DIGITAL HIGHWAY,

encapsulated in the D3S endeavour,  
has already become one of the priority  
interconnection projects of the Three  
Seas Initiative.

**#Digital3Seas**



THE KOSCIUSZKO INSTITUTE

# 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](http://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 €**



### 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
- Military & 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**