VOLUME 3 (2017) ▪ ISSUE 1

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.

ISSN: 2450-21113

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

THE KOSCIUSZKO INSTITUTE

Citations: This journal should be cited as follows:
"European Cybersecurity Journal",
Volume 3 (2017), Issue 1, page reference

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

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

www.ik.org.pl
www.cybersecforum.eu

Printed in Poland
by Drukarnia Diament | diamentdruk.pl

DTP: Marcin Oroń

EDITORIAL

DR JOANNA ŚWIĄTKOWSKA
Chief Editor of the European Cybersecurity Journal
CYBERSEC Programme Director
Senior Research Fellow of the Kosciuszko Institute, Poland

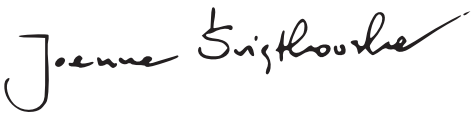
When the Kosciuszko Institute approached some experts to enquire about their predictions for cybersecurity trends in 2017, they were in agreement on at least a few points. The year that has just begun will bring both the increased offensive activity of states in cyberspace and the intensified activity of terrorists using the Internet to conduct their sinister operations.

Both trends pose a very serious threat to the stability of the entire international security system. Conflicts in cyberspace can very easily escalate to a level entailing even the deployment of kinetic measures. Terrorists, in turn, once they have mastered the art of launching successful cyberattacks, can wreak catastrophic damage. Unlike others, they stop at nothing, aiming to do as much harm as possible.

This edition of ECJ features two texts analysing the above-mentioned problems. The article devoted to cyber confidence building measures traces the history of the development of stabilization and trust-enhancing tools which – if successfully applied – have the chance to reduce the occurrence of events with grave implications for the international community. The article about the use of Twitter and Telegram by terrorists provides a valuable insight into the activities these groups presently undertake on the Internet. Both texts have the potential to inspire decision-makers to take action in order to strengthen global security and stability.

This issue of ECJ conveys a great deal of practical knowledge related to cybersecurity. It presents concrete instruments such as cyber insurance policies or active defence models that will certainly deepen our understanding of how our online security can be increased.

This is but a small sample of topics covered in this edition of our journal. Enjoy the read and broaden your horizons. In these increasingly tense and unstable times, such knowledge might actually come in handy.



CONTENTS

SPEECH BY COMMISSIONER JULIAN KING

SIR JULIAN KING
Sir Julian King was appointed Commissioner for Security Union on the 19th September 2016. He joined the Foreign & Commonwealth Office in 1985. He has held various positions, including: UK Ambassador to France (2016); Director General Economic & Consular (2014); DG of the Northern Ireland Office London and Belfast (2011); UK Ambassador to Ireland (2009); EU Commission Chef de Cabinet to Commissioner for Trade (2008); UK Representative on EU Political and Security Committee, (2004). Sir Julian is a graduate of Oxford University. He was awarded the KCVO in 2014; CVO in 2011 and CMG in 2006.

Speech by Commissioner King at the 4th Annual European Cyber Security Conference in Brussels (17.11.16)

Three weeks ago, a Distributed Denial of Service attack took down Dyn, a central name service provider, disabling access to Twitter, SoundCloud, Spotify, Reddit and a number of other popular services for hours at a time. The attack managed to reach unprecedented size by harnessing the collective firepower of so-called Internet of Things devices – often poorly secured printers, security cameras, digital video recorders or other tools that are connected to the internet for remote access and control by their users.

Now I am not a digital native. So I was surprised to discover that pretty much anyone – including me – could have perpetrated this attack. The malware that was used to create the botnet is available for free online. Or – instead of building my own botnet – I could have simply rented a ready-made botnet by the hour at very affordable rates and specified my target in the easy-to-use interface. In fact, rented botnets were used in the attack. But let me assure you – it wasn't me.

Now why am I telling you this story? It illustrates some of the key weaknesses of our system.

First of all, name services such as Dyn are not recognized as a critical infrastructure. And yet when they go down the sites that they provide services for are rendered inaccessible. So we clearly still have work to do in making our laws 'technology neutral'.

Secondly, a lot of the devices that were used for the attack have their user name and password hard coded. That means that users cannot change them even if they were savvy enough to realize the need to do so. It is the equivalent of a wide-open door for anyone wanting access. This shows that we have a long way to go in security by design.

And third, it shows our dependence on private actors for key services. While most of us can survive a day without access to Twitter or SoundCloud, such an attack could also affect web-based services that are of greater critical importance to our daily lives. And as our reliance on the Internet increases, so does our vulnerability. We benefit from the vast potential of the Internet, but we also expose ourselves to threats. In connecting ourselves, we give up control over our vulnerabilities and put ourselves at the mercy of the vulnerabilities of the weakest link in the chain – which we don't control.

The uncomfortable truth is that Europe is currently facing an unprecedentedly high and growing level of cyber threat originating from hostile state and non-state actors who are skilled at exploiting these vulnerabilities. The most acute threat stems from cyber-espionage from hostile states. However, we also face the threat of destructive cyber-attacks from capable state and non-state actors, such as cyber-criminals and political hacktivists. Such attacks fall into the category of hybrid threats. The most technically advanced, persistent and aggressive threats are aimed manipulating public opinion particularly during election campaigns in order to destabilise or undermine and it is safe to assume that such attacks will continue to be used to try to influence elections in Europe in 2017.

Tackling the threat requires concerted, collective action to build resilience, to contain threats, to mitigate the impact of successful attacks, and to respond to them. The Commission is playing an active part in this work.

Cyber security has been at the heart of this Commission's political priorities and is a central element of the Digital Single Market Strategy, while the fight against cybercrime is one of the three pillars of the 2015 European Agenda on Security.

> “ Europe is currently facing an unprecedentedly high and growing level of cyber threat originating from hostile state and non-state actors who are skilled at exploiting these vulnerabilities.

Cybersecurity matters. An old adage has it that there are only two types of companies in the world; those that know they've been hacked, and those that don't. Just to give you one recent example, half of businesses in EU Member States have already experienced a successful ransomware attack.

> “ Half of businesses in EU Member States have already experienced a successful ransomware attack.

The response cannot be to disconnect. Instead, it must be based around three pillars: strengthening the fight against cybercrime through increased cooperation and a reinforced legal framework; strengthening resilience against cyberattacks; and promoting and supporting technological innovation including by making use of the EU's research funds to drive new solutions and to create new technologies.

Strengthening the fight against cybercrime

1) Through increased cooperation: the role of EU agencies

With regards to cooperation, the European Cybercrime Centre (EC3) at Europol has already become a central hub in the network of actors fighting cybercrime. Two good examples of successful cross-border and cross-sector cooperation in the fight against cybercrime illustrate that; just last month, the EC3 supported an operation resulting in the detention of 193 individuals for having travelled with tickets bought using stolen credit cards. 43 countries, 75 airlines and 8 online travel agencies were involved in this global operation which took place at 189 airports across the world.

A further example is the work EC3 has been doing with the Dutch National Police and Kaspersky on Ransomware – malware introduced into a computer forcing its owner to pay a ransom to get their data back. The 'No More Ransom' initiative provides victims with free advice and decryption tools that can recover information encrypted with one of seven ransomware strands. More than 2500 devices have already been successfully decrypted for free.

We need to improve and expand our cooperation. Eurojust has a key role to play when it comes to supporting and linking national judicial authorities in the fight against

cybercrime. Eurojust has taken a key step towards reinforced cooperation by volunteering to support the new European Judicial Cybercrime Network. This network will hold its kick-off meeting in a week, on 24 November. We hope that it will help bring cooperation between Member States' judiciary authorities to a new level.

And we have many budding public-private partnerships at national level, like the UK Global Cyber Alliance or the German Allianz für Cybersicherheit (Cybersecurity Alliance). At EU level, the work that the EC3 has been doing with its private sector advisory groups has opened up new possibilities for more effective law enforcement. Conferences and other initiatives organised jointly by the EC3, ENISA, CERT-EU and other agencies have brought together actors across communities and facilitated both strategic and operational cooperation. We need to expand and build on these efforts. As mentioned before, the private sector is the key partner for law enforcement and such cooperation is essential.

2) Through a reinforced common legal framework

In the fight against cyber-enabled criminal or terrorist act, digital evidence has become key as it is often the only existing lead.

Access to digital evidence is essential for criminal investigations; however, it is often difficult to obtain as it is stored on servers operated by private service providers often outside the jurisdiction of the investigating law enforcement agency. The Commission has launched an expert process to help identify options. The Commission also plans to improve Mutual Legal Assistance by simplifying and accelerating requests. Other existing mechanisms to obtain cross-border access to electronic evidence also need to be improved, including direct cooperation with service providers.

We also need to make sure that internet-based communication services providers, so-called OTTs (over-the-top service providers) have the same obligations as the telecom operators, particularly concerning cooperation with law enforcement authorities regarding criminal investigations. This is why the Commission intends to present a revised e-privacy Directive early next year. It will help level the playing field and align the scope to that already adopted in the telecoms package.

Reinforcing cyber security and increasing cyber-resilience across the EU

A key part of our response to cyber threats must be based on identifying and closing off vulnerabilities making the EU a much less attractive target. The recently adopted Network and Information Security Directive lays the groundwork for improved EU level cooperation and cyber resilience. The framework is designed to support and facilitate strategic cooperation and the exchange of information among Member States, and to promote operational cooperation on specific cyber security incidents and sharing information about risks. Under the directive, Member States have to identify businesses of strategic importance for society and the economy and ensure that they take appropriate cyber security measures and notify serious incidents to the relevant national authority.

We now need to work together to ensure swift implementation of the NIS Directive, covering all relevant actors. As the Dyn attack shows, it is easy to overlook actors that are close to invisible in daily operations but essential to the functioning of the internet.

The private sector has an important role to play in standard-setting through the NIS Platform and other mechanisms. Security by design, including for the Internet of Things and devices such as those abused for the attack on Dyn, is just one of many topics that it has already covered.

Promoting and supporting technological innovation

Our close cooperation with the private sector can also help advance and strengthen the EU cyber security sector. In July the Commission launched a €1.8 billion Public Private Partnership on cyber security with industry. The EU is investing €450m with cyber security market players – and I see many of you in the room here today – represented by the European Cyber Security Organisation (ECSO) expected to invest three times this

figure. The partnership also includes representatives of national administrations. The aim is to help drive technological innovation and solutions for key sectors such as energy, health, transport and finance.

In parallel, the European Commission is working to strengthen industrial capabilities in Europe, by addressing the current cyber security market fragmentation. The European Defence Action Plan will be presented to the Council of Ministers in early December. It will be coupled with a new European Defence Research Programme, focusing on defence research and development using the EU budget for the first time. These initiatives reflect the European Commission's enabling and facilitating role for a competitive European defence industry and European defence cooperation.

Beyond these large-scale initiatives, the Commission has also taken steps to make sure that Horizon2020 funding is available to support smaller projects. Future calls and the next annual programmes should have a heightened focus on counter-terrorism technology and capabilities, drawing on the work of the European Counter Terrorism Centre, the European Cybercrime Centre as well as national law enforcement and intelligence communities. Cybercrime in particular is an exponentially evolving problem requiring coordinated action of law enforcement authorities, policy makers, industry and researchers. As such, cybercrime is a priority area in the Fighting Crime and Terrorism strand of Horizon 2020.

Creating effective cyber security, from the micro-level of one app or one device – such as the cameras and video recorders used in the attack on Dyn – to the macro-level of an entire organisation or beyond is a challenge no country and no sector can face alone. So we look to you, the private sector, to give us new ideas and to develop new solutions to the common challenge we all face together. I look forward to your discussion today on these issues, and to the outcome of this 4th EU Cyber Security Conference, as we work together to address cybercrime and cyber security issues across Europe in a more effective manner. ■

Our business
is to care for your business

Work with a solid partner you can rely on.
Choose PZU – the leading insurer in Poland and Central and Eastern Europe.

Contact us

801 102 102 **pzu.pl**

Calls are charged in accordance with the operator's tariff

POLICY REVIEW

BUILDING CONFIDENCE IN THE CYBER REALM AS A MEANS OF PREVENTING CONFLICT – A SWISS PERSPECTIVE

PROF. SOLANGE GHERNAOUTI
is director of the Swiss Cybersecurity Advisory and Research Group – University of Lausanne. She holds a PhD in Computer Science (Paris University), is former auditor of the French Institute of Advanced Studies in National Defence, Associate Fellow at the Geneva Center for Security Policy, member of the UNESCO Swiss Commission and of the Swiss Academy of Technical Sciences. She has authored more than 300 publications and thirty books including "Cyberpower: Crime, Conflict and Security in Cyberspace" (EPFL press 2013). She is Chevalier de la Légion d'Honneur and has been recognised by the Swiss press as one of the outstanding women in professional and academic circles.

LAURA CRESPO
is a researcher at the University of Lausanne, where she is currently writing her dissertation on Switzerland's role regarding the international normative debate in the cyber realm. Furthermore, Ms. Crespo works at the Swiss Federal Department of Foreign Affairs. She has been involved in the implementation of the national Swiss cyber strategy and she has been engaged in different international processes regarding cyber-security, in particular the process within the OSCE on confidence building measures. Prior to that she worked at the Project Cyber Defence within the Federal Department of Defence, Civil Protection and Sport.

1. Introduction

Cyberthreats affect systems critical to national security, the state, its interests and its underlying values, making them one of the most salient topics of high-level politics[1]. As new technologies are increasingly being developed for offensive and defensive purposes, the rising number and sophistication of cyberattacks have had destabilising effects on international peace, stability and security.

> "The militarisation of cyberspace has had a global impact on states, including on the way they cooperate and interact with one another.

In fact, the linking of mass-information and communication technologies to national security concerns has existed since the Internet's inception[2]. And yet, the international community has only recently devoted significant resources to the development of an international diplomatic and security agenda. Dialogue and debate on cyberspace and the security matters pertaining to it are occurring at the global, regional and bilateral levels. The militarisation of cyberspace has had a global impact on states, including on the way they cooperate and interact with one another. Moreover, accelerated by strong media coverage, this development has emphasised the need to create a normative framework – a rulebook for cyberspace. What are the guiding principles that should structure state behaviour in cyberspace? What actions are appropriate for states when they use information and communication technologies? What are their constraints? Policymakers in fora such as the United Nations (UN) and the Organization for Security and Cooperation in Europe (OSCE) have recently devoted considerable time to developing norms of responsible state behaviour and confidence-building. Still, despite their progress, a normative international framework remains inchoate.

1 | Choucri N. and Clark D., Cyberspace and International Relations. Toward an Integrated System, 2011 (online) http://ecir.mit.edu/images/stories/Salience%20of%20Cyberspace%208-25.pdf (access: 03.03.2015).

2 | Dunn Cavelty M., Cyber-Security and Threat Politics: US Efforts to Secure the Information Age, London Routledge, 2008.

At national level, Switzerland now finds itself in the midst of a debate on which rules for responsible state behavior should be in force and the overall form they should take. Unlike other policy areas (e.g., Swiss bilateral relations with the European Union) where it is often labeled a "special case" (Sonderfall)[3], Switzerland is actively committed to increasing cybersecurity by promoting globally shared guidelines for this domain. At the 2015 Global Conference on Cyberspace in The Hague, Swiss Federal Department of Foreign Affairs Head Didier Burkhalter stated that any such normative framework "must be based on the existing international legal order and trust to ensure an open, free and secure cyberspace"[4].

How has Switzerland contributed to the international debate regarding cybersecurity? Answering this question will be at the core of this article. With this in mind, attention will be paid to the process of confidence-building measures (CBMs) within the OSCE. First, the instrument of CBMs will be defined and contextualised. Second, the authors seek to outline the path the regional security organization has taken to adopt a holistic approach regarding cybersecurity. Third, the article illustrates the process leading towards the adoption of a set of measures designed to enhance transparency and increase interstate cooperation, which in turn paves the way for stabilising the cyber domain. The fourth part of this article is devoted to the role Switzerland has played in shaping the OSCE cyber agenda by providing a Swiss perspective on the OSCE process.

Confidence-Building Measures: Definition and Contextualisation

Building confidence is a strong component in the contextual environment of peace and security. To develop a sustainable security and peace regime, CBMs are acknowledged as powerful facilitators of transparency and predictability. Confidence reduces deep-seated mutual suspicions, concerns and fears. Building confidence is a gradual process based on reciprocity and continuity. In the development of constructive and durable relationships, a culture of "give-and-take" is necessary to dispel mistrust[5].

Although the instrument of CBMs was developed for universal use, its origin is the European theatre[6]. During the Cold War and post-Cold War periods, the European political-military environment was characterised by confrontation and division. The core purpose of the concept and development of CBMs was to strengthen stability in a "frozen status quo" and thus minimise the danger of a surprise attack and mass warfare in Europe[7]. Therefore, this policy model was mainly designed to stabilise East-West relations during and after the Cold War.

Johan Jørgen Holst[8] maintains that CBMs were developed up to the 1980s to "inhibit the political exploitation of military force". Afterwards, they were presumably designed to "reduce the danger of surprise attack"[9]. In his conceptual framework for this policy model, he defined CBMs as "arrangements designed to enhance (...) assurance of mind and belief in the trustworthiness of states and the facts they create"[10]. Susan Pederson and Stanley Weeks[11] provide a narrower definition, referring to "practices of arms control and other measures taken by the competing Soviet and Western Blocs"[12]. Consequently, most of the measures conducive to building confidence were, at least in the beginning, intended

3 | Church C., The Paradoxical Europeanisation of Switzerland "European Business Journal", 8 (2), 1996, 9-17; Church C. H., Politics and Government of Switzerland, 2004, Basingstoke: Palgrave Macmillan; Gstöhl S., The EU Response to Switzerland: Still a "Special Case"? In: Church C. H., Switzerland and the European Union: A Close, Contradictory and Misunderstood Relationship, 2007, New York: Routledge.

4 | Burkhalter D., Promoting trust and globally shared rules to ensure an open, free and secure cyberspace, 2015 (online) https://www.news.admin.ch/message/index.html?lang=de&msg-id=56892 (access: 30.05.2015).

5 | Lachowski Z., Confidence- and Security Building Measures in the New Europe, SIPRI Research Report No. 18, 2014, Oxford University Press.

6 | Ibid.

7 | Ibid p.1.

8 | Holst J.J., Confidence-building measures: a conceptual framework, "Survival", 25 (1), 1983.

9 | Ibid p.2.

10 | Ibid p.2.

11 | Pederson S. and Weeks S., A Survey of Confidence Building Measures, In: Cossa R. A., Asia Pacific Confidence and Security Building Measures, Washington DC: The Center for Strategic Studies and International Studies, 1995.

12 | Ibid p.82.

for the military realm. The first examples of CBMs were, therefore, the implementation of verification mechanisms to control arms, along with the establishment of military communication channels and military transparency.

East-West détente led to the 1975 signing of the Helsinki Final Act at the Conference on Security and Cooperation. For the first time, a set of principles and rules of conduct codified the goals of CBMs. The founding document of the Conference on Security and Co-operation in Europe, the Helsinki Final Act, described CBMs as an instrument "to contribute to reducing the dangers of armed conflict and of misunderstanding or miscalculation of military activities which could give rise to apprehension, particularly in a situation where states lack clear and timely information"[13] (CSCOE, 1975). Even though a common definition of CBMs is still lacking, their underlying rationale is to reinforce stability, thereby reducing the danger of a sudden, unexpected, large-scale armed attack.

> "CBMs underlying rationale is to reinforce stability, thereby reducing the danger of a sudden, unexpected, large-scale armed attack.

The OSCE-Process on CBMs: Towards a Comprehensive Cyber Approach

The OSCE is a regional body employing a comprehensive approach to security. Dealing with security matters across politico-military, economic/environmental, and human dimensions, it offers an inclusive platform for dialogue between 57 participating Euro-Atlantic and Eurasian states. As a security organization, the OSCE is known for finding common solutions based on cooperation and political commitment. It operates on the basis of consensus, which sometimes makes negotiation challenging. However, considering its record developing and implementing CBMs regarding conventional arms control (e.g. the Stockholm and Vienna documents), the participating States agreed to add cybersecurity to the OSCE's mandate.

> "The Astana Declaration marked the beginning of a new OSCE era: the participating States adopted a resolution on cybersecurity and cybercrime.

Initially, the OSCE dealt on a case-by-case basis with cybersecurity threats, e.g., cybercrime and the use of the Internet for terrorist purposes. In 2008, though, with the Astana Declaration of the OSCE Parliamentary Assembly, the OSCE member States abandoned this approach, opting instead for a strategy aimed at the full gamut of cyber risks. The Astana Declaration marked the beginning of a new OSCE era. For the first time, the participating States adopted a resolution on cybersecurity and cybercrime "recognising that cyberattacks can be a great challenge to governments, because they may destabilise society, jeopardise the availability of public services and the functioning of vital infrastructure"[14]. While reaffirming the OSCE's role as "a regional arrangement under Chapter VIII of the UN Charter and a key instrument for early warning, conflict prevention, crisis management and post-conflict rehabilitation in its area"[15], the Astana Declaration recognised previous OSCE success regarding "various aspects of cybersecurity and cybercrime, and in particular related to terrorist use of the Internet"[16]. Still, cybercrime and cyberterrorism were treated as separate activities. Gradually, the OSCE's participating States acknowledged that interrelationships between many cyberthreats called for a still

13 | Conference on Security and Co-Operation in Europe Final Act, 1975, p. 10. (online) https://www.osce.org/mc/39501?download=true (access: 11.11.2015).

14 | OSCE Parliamentary Assembly, Astana Declaration of the OSCE Parliamentary Assembly and Resolutions Adopted at the Seventeenth Annual Session, 2008 (online) https://www.oscepa.org/documents/all-documents/annual-sessions/2008-astana/declaration-7/256-2008-astana-declaration-eng/file (access: 02.12.2015).

15 | Ibid paragraph 8, p.13.

16 | Ibid paragraph 10, p.13.

broader focus. In March 2009, the "OSCE Workshop on a Comprehensive OSCE Approach to Enhancing Cybersecurity"[17] was conducted "[to define] a possible role for the OSCE in (...)a comprehensive approach to enhancing cybersecurity, and identify concrete measures for possible follow-up action by all relevant OSCE bodies." In his opening statement at the Workshop, French Ambassador Eric Lebédel recalled the OSCE security credo, enshrined in the 1994 "Code of Conduct on Politico-Military Aspects of Security," that "security is indivisible and that the security of each (...) [participating State] is inseparably linked to the security of all others"[18]. As cyber risks clearly affected all OSCE members, the workshop concluded that the full range of cybersecurity issues should be placed on the OSCE's agenda.

In 2010, the Oslo Declaration of the OSCE Parliamentary Assembly reiterated the need to increase interstate cooperation to cope with cybercrime and other "modern security risks"[19]. Following the 2010 release of the report of the UN Group of Governmental Experts on Develop ments in the Field of Information and Telecommunications in the Context of International Security (UN GGE)[20], the Lithuanian Chairmanship of the OSCE and the OSCE Secretariat of the Transnational Threat Department organised a conference to explore the OSCE's future role[21]. Primarily targeting political decision-makers of national cybersecurity authorities, the 2011 conference scrutinised how the OSCE could "add value to existing efforts through a comprehensive approach to cybersecurity including the exchange of views at national level and potentially developing norms relevant to the behavior of States in cyberspace."

Considering the general agreement among participating States, it was argued that the OSCE "offers a unique platform to discuss threats to cybersecurity due to its comprehensive approach to security and membership"[22]. The recommendations formulated during the two-day conference included a suggestion that the OSCE "focus on measures related to the politico-military dimension" and apply its "expertise regarding CBMs in cyberspace to enhance transparency, predictability, stability, and reduce the risk of misperception and escalation of conflict"[23]. The participating States also "recognised that cyberspace is linked to the politico-military domain, including to critical infrastructures and that national security is intrinsically linked with cybersecurity"[24].

In 2012, under Irish Chairmanship, in Decision 1039[25], the OSCE Permanent Council established an "open-ended, informal OSCE working group which should operate under the auspices of the Security Committee". Informal working group 1039 (IWG 1039) was mandated to "elaborate a set of draft CBMs to enhance interstate

17 | OSCE Forum for Security Co-operation, OSCE Workshop on a Comprehensive OSCE Approach to Enhancing Cyber Security, FSC. DEC/10/08, 2008 (online) http://www.osce.org/fsc/34759?download=true (access: 03.12.2015).

18 | OSCE, Code of Conduct on Politico-Military Aspects of Security. DOC.FSC/1/95, 1994, (online) https://www.osce.org/fsc/41355?download=true (access: 04.12.2015).

19 | OSCE Parliamentary Assembly, Oslo Declaration of the OSCE Parliamentary Assembly and Resolutions Adopted at the Nineteenth Annual Session, 2010 (online) https://ccdcoe.org/sites/default/files/documents/OSCE-100710-OsloDeclarationandResolutions.pdf (access: 02.12.2015).

20 | United Nations, General Assembly, A/65/201, 2010, Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security, (online) http://www.unidir.org/files/medias/pdfs/information-security-2010-doc-2-a-65-201-eng-0-582.pdf (access 01.12.2015).

21 | OSCE Permanent Council, PC.DEC/992. Agenda, Timetable and Organizational Modalities for the OSCE Conference on a Comprehensive Approach to Cyber Security: Exploring the Future OSCE Role, 2011, (online) http://www.osce.org/pc/76454?download=true (access 05.12.2015).

22 | OSCE, OSCE Conference on a Comprehensive Approach to Cyber Security: Exploring the Future OSCE Role. Closing Remarks by H.E. Ambassador Norkus, Chairperson of the OSCE Permanent Council. CIO.GAL/87/11, 2011, (online) http://www.osce.org/cio/77481?download=true (access 05.12.2015).

23 | Ibid p.2.

24 | OSCE Permanent Council, PC.GAL/67/11. OSCE Conference on a Comprehensive Approach to Cyber Securi-ty: Exploring the Future OSCE Role, 2011, (online) http://www.osce.org/cio/77317?download=true (access 07.12.2016).

25 | OSCE Permanent Council, Development of Confidence-Building Measures to Reduce the Risks of Conflict Stemming from the Use of Information and Communication Technologies. PC.DEC/1039, 2012 (online) http://www.osce.org/pc/90169 (access 07.12.2015).

co-operation, transparency, predictability, and stability, and to reduce the risks of misperception, escalation, and conflict that may stem from the use of ICTs"[26].

Towards the Adoption of the First Set of CBMs in Cyberspace

IWG 1039 met under the US Chair three times before the Irish OSCE Ministerial Council met in December 2012. For the first meeting, convened in July 2012, the US had – in collaboration with other OSCE delegations – developed a list of more than 50 confidence-building measures[27]. The proposed preliminary measures were intended to lead towards "the foundation of international ICT stability"[28]. The Chair outlined the rationale of CBMs, a three-level approach beginning with increased transparency, which would enhance confidence and predictability. The second level would involve cooperative measures to prevent or respond to disruptive activities and any crises they might precipitate. Building on these and other cooperative measures, stability would result from reframing state behavior to counter "destabilising activities"[29]. Each level of development would both complement and presuppose the other.

IWG 1039 convened a second time in October 2012, and again the following month. The main objective of these meetings was to narrow the list of more than 50 proposed confidence-building activities to a set of six that would maximise transparency and predictability. The "Best Guess"[30] draft negotiated at that time proposed six CBMs, namely exchanging national views and best practices on national cybersecurity strategies and sharing information on national organizations, structures and programmes devoted to securing cyberspace. It further proposed establishing high-priority points of contact ("communication hotlines") between policymakers and their technical operatives to ensure communication between states and to coordinate responses, especially in the event of a major disruptive incident. To reduce misunderstandings, the exchange of national terminologies and the development of an international registry of national definitions of key concepts were suggested. Exploring OSCE's means for communication and the group's modalities were further formulated in CBMs.

From the outset of the OSCE process on CBMs, the majority of the participating States backed the paper offered by the IWG Chair and the US delegation. Most delegations saw added value in starting with the "low-hanging fruits," including the six activities selected as first-level CBMs, which could be easily implemented and would encounter little, if any, resistance. Initially increasing transparency by exchanging information and best practices on cyber strategies, developing points of contact and an OSCE-wide registry of national terminologies was also perceived by most as an adequate, politically feasible approach.

Consequently, at the 2012 Ministerial Council in Dublin, the above-mentioned draft of six measures was tabled for a Ministerial Council decision on CBMs to reduce the risks of conflict stemming from the use of ICTs. However, in spite of general support as well as the voluntary and non-binding character of the measures, no decision was reached[31].

In 2013, Ukraine took over the OSCE Chairmanship, declaring an agreement on CBMs one of the body's top priorities. Generally characterised by constructive debates and negotiations, the discussions illustrated the delegations' willingness to find common ground on matters that had previously divided Eastern and

26 | Ibid.

27 | OSCE Parliamentary Assessment, General Committee on Political Affairs and Security. Follow-Up on Recom-mendations in the OSCE PA's Monaco Declaration. Final Report for the 2013 Annual Session, 2013 (online) https://www.oscepa.org/documents/all-documents/annual-sessions/2013-istanbul/follow-up-report-3/1782-2013-annual-session-follow-up-final-report-1st-committee-english/file (access 07.12.2015).

28 | Ibid p.9.

29 | Ibid p.9.

30 | OSCE, United States Mission to the OSCE; Informal Working Group Established by PC Decision 1039: Revised Draft Set of CBMs. PC. DEL/871/12/Rev.1, 2012 (online) https://cryptome.org/2013/03/osce-cbms.pdf (access 07.12.2015).

31 | OSCE Parliamentary Assessment, General Committee on Political Affairs and Security. Follow-Up on Recom-mendations in the OSCE PA's Monaco Declaration. Final Report for the 2013 Annual Session, 2013 (online) https://www.oscepa.org/documents/all-documents/annual-sessions/2013-istanbul/follow-up-report-3/1782-2013-annual-session-follow-up-final-report-1st-committee-english/file (access 07.12.2015).

Western countries. The same year, the bilateral agreement between the US and the Russian Federation and the publication of the UN GGE report[32] both helped create an environment of cooperation and fruitful dialogue.

Under Ukraine's OSCE Chairmanship and at the last IWG 1039 meeting in November 2013, the participatingStates managed to find a consensus on a total of eleven initial measures designed to increase confidence and trust in the digital domain and "reduce the risk of conflict stemming from the use of information and communication technologies"[33]. The initial set was then formally adopted by the OSCE Permanent Council on 3 December 2013.

DECISION No. 1106 Initial Set of Confidence-Building Measures to Reduce the Risks of Conflict Stemming from the Use of Information and Communication Technologies	
CBM 1	Participating States will voluntarily provide their national views on various aspects of national and transnational threats to and in the use of ICTs. The extent of such information will be determined by the providing Parties.
CBM 2	Participating States will voluntarily facilitate co-operation among the competent national bodies and exchange of information in relation with security of and in the use of ICTs.
CBM 3	Participating States will on a voluntary basis and at the appropriate level hold consultations in order to reduce the risks of misperception, and of possible emergence of political or military tension or conflict that may stem from the use of ICTs, and to protect critical national and international ICT infrastructures including their integrity.
CBM 4	Participating States will voluntarily share information on measures that they have taken to ensure an open, interoperable, secure, and reliable Internet.
CBM 5	The participating States will use the OSCE as a platform for dialogue, exchange of best practices, awareness-raising and information on capacity-building regarding security of and in the use of ICTs, including effective responses to related threats. The participating States will explore further developing the OSCE role in this regard.
CBM 6	Participating States are encouraged to have in place modern and effective national legislation to facilitate on a voluntary basis bilateral co-operation and effective, time-sensitive information exchange between competent authorities, including law enforcement agencies, of the participating States in order to counter terrorist or criminal use of ICTs. The OSCE participating States agree that the OSCE shall not duplicate the efforts of existing law enforcement channels.
CBM 7	Participating States will voluntarily share information on their national organization; strategies; policies and programmes – including on co-operation between the public and the private sector; relevant to the security of and in the use of ICTs; the extent to be determined by the providing parties.
CBM 8	Participating States will nominate a contact point to facilitate pertinent communications and dialogue on security of and in the use of ICTs. Participating States will voluntarily provide contact data of existing official national structures that manage ICT-related incidents and co-ordinate responses to enable a direct dialogue and to facilitate interaction among responsible national bodies and experts. Participating States will update contact information annually and notify changes no later than thirty days after a change has occurred. Participating States will voluntarily establish measures to ensure rapid communication at policy levels of authority, to permit concerns to be raised at the national security level.

32 | United Nations General Assembly, A/68/98, 2013, Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security. (online) http://www.unidir.org/files/medias/pdfs/developments-in-the-field-of-information-and-telecommunications-in-the-context-of-international-security-2012-2013-a-68-98-eng-0-578.pdf (access 01.12.2015).

33 | United Nations General Assembly, A/68/98, 2013, Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security. (online) http://www.unidir.org/files/medias/pdfs/developments-in-the-field-of-information-and-telecommunications-in-the-context-of-international-security-2012-2013-a-68-98-eng-0-578.pdf (access 01.12.2015).

CBM 9	In order to reduce the risk of misunderstandings in the absence of agreed terminology and to further a continuing dialogue, participating States will, as a first step, voluntarily provide a list of national terminology related to security of and in the use of ICTs accompanied by an explanation or definition of each term. Each participating State will voluntarily select those terms it deems most relevant for sharing. In the longer term, participating States will endeavour to produce a consensus glossary.
CBM 10	Participating States will voluntarily exchange views using OSCE platforms and mechanisms inter alia, the OSCE Communications Network, maintained by the OSCE Secretariat's Conflict Prevention Centre, subject to the relevant OSCE decision, to facilitate communications regarding the CBMs.
CBM 11	Participating States will, at the level of designated national experts, meet at least three times each year, within the framework of the Security Committee and its Informal Working Group established by Permanent Council Decision No. 1039 to discuss information exchanged and explore appropriate development of CBMs. Candidates for future consideration by the IWG may include inter alia proposals from the Consolidated List circulated by the Chairmanship of the IWG under PC.DEL/682/12 on 9 July 2012, subject to discussion and consensus agreement prior to adoption.

This set of CBMs was the first of its kind to be adopted by a regional security organization such as the OSCE. In addition to the OSCE itself, other regional security organizations (e.g., the ASEAN Regional Forum) and the international community as a whole saw this as an important breakthrough towards improved interstate cooperation, increased transparency and predictability, and stability in the use of ICTs. It was also interpreted as an expression of the political will of states to anchor cybersecurity in the multilateral agenda.

Implementing the First Set of CBMs and Developing a Second Set

The OSCE's agenda for 2014 was shaped by a dual-focus approach: delegations agreed to implement the existing CBMs while concurrently exploring potential additions. The 2014 implementation of the first set of CBMs as adopted in Decision No. 1106 of the OSCE Permanent Council coincided with the Swiss OSCE Chairmanship. Unfortunately, it also coincided with the outbreak of the conflict between Ukraine and the Russian Federation. Considering the complexity of its member states' geopolitical constellation, the annexation of Crimea clearly jeopardised the OSCE's progress on CBMs in cyberspace. However, it also stress-tested the OSCE's capability as a regional organization to prevent and manage conflict.

Notably, the participating States regarded the implementation process as an opportunity to show-case their work at national and international level. For the first time, all 57 participating States, and not only the major powers, could voice their concerns and share their views. More importantly, the OSCE's CBMs provided ideal opportunities for states relatively new to the cybersecurity discussion to interact with those with mature cybersecurity systems. Therefore, OSCE IWG 1039 developed as a mutually beneficial forum conducive to building capacity for countries with lower expertise. Viewed as a success in itself, the implementation process produced a remarkable outcome, as the participating States proved willing first to make, then to honour OSCE commitments. With dialogue, interaction and commitment contributing to mutual understanding, their high degree of participation epitomised the OSCE's credo of cooperative security.

> "The OSCE's CBMs provided ideal opportunities for states relatively new to the cybersecurity discussion to interact with those with mature cybersecurity systems.

At the same time, states launched discussions on a second set of CBMs. Very soon, new proposals would provide another milestone on the OSCE's path toward increased cyberspace predictability and stability. Acknowledging that the bar was set very high, a number of delegations emphasised the need to focus on a modest, realistic and practical second set of CBMs.

However, many of their proposals fit very well with the concept of building confidence via inter-state cooperation. Examples tabled during the capital-expert meetings included the organization of workshops and seminars to address issues involving the private sector and academic community, and visits to centres of excellence regarding cybersecurity.

Towards the Adoption of Additional Five CBMs in Cyberspace

In February 2016, two years after the adoption of the initial eleven CBMs, IWG 1039 again managed to find consensus on a second set of five. The Permanent Council formally adopted these on 10 March 2016[34]. While the first set of CBMs focused on increasing transparency and thereby enhancing the predictability of a state's behaviour, the second set of five CBMs aims at advancing the state-to-state relations in the digital domain.

"While the first set of CBMs focused on increasing transparency and thereby enhancing the predictability of a state's behaviour, the second set of five CBMs aims at advancing the state-to-state relations in the digital domain.

DECISION No. 1202 **OSCE Confidence-Building Measures to Reduce the Risks of Conflict stemming from the Use of Information and Communication Technologies**	
CBM 12	Participating States will, on a voluntary basis, share information and facilitate inter-State exchanges in different formats, including workshops, seminars, and roundtables, including on the regional and/or subregional level; this is to investigate the spectrum of co-operative measures as well as other processes and mechanisms that could enable participating States to reduce the risk of conflict stemming from the use of ICTs. Such activities should be aimed at preventing conflicts stemming from the use of ICTs and at maintaining peaceful use of ICTs.
CBM 13	Participating States will, on a voluntary basis, conduct activities for officials and experts to support the facilitation of authorized and protected communication channels to prevent and reduce the risks of misperception, escalation, and conflict; and to clarify technical, legal and diplomatic mechanisms to address ICT-related requests. This does not exclude the use of the channels of communication mentioned in Permanent Council Decision No. 1106.
CBM 14	Participating States will, on a voluntary basis and consistent with national legislation, promote public-private partnerships and develop mechanisms to exchange best practices of responses to common security challenges stemming from the use of ICTs.
CBM 15	Participating States, on a voluntary basis, will encourage, facilitate and/or participate in regional and subregional collaboration between legally-authorized authorities responsible for securing critical infrastructures to discuss opportunities and address challenges to national as well as transborder ICT networks, upon which such critical infrastructure relies.
CBM 16	Participating States will, on a voluntary basis, encourage responsible reporting of vulnerabilities affecting the security of and in the use of ICTs and share associated information on available remedies to such vulnerabilities, including with relevant segments of the ICT business and industry, with the goal of increasing co-operation and transparency within the OSCE region. OSCE participating States agree that such information exchange, when occurring between States, should use appropriately authorized and protected communication channels, including the contact points designated in line with CBM 8 of Permanent Council Decision No. 1106, with a view to avoiding duplication.

34 | OSCE, OSCE Confidence-Building Measures to Reduce the Risks of Conflict Stemming from the Use of Infor-mation and Communication Technologies. PC.DEC/1202, 2016 (online) http://www.osce.org/pc/227281?download=true. (access 20.03.2016).

Switzerland in the OSCE Process on Confidence-Building in Cyberspace: Its Role, Engagement and Commitment

On 27 June 2012, the Swiss Federal Council (Bundesrat) adopted a national cybersecurity strategy titled the "National strategy for Switzerland's protection against cyber-risks"[35]. Along with a number of states that developed and published national cybersecurity strategies from 2009-2014, Switzerland recognises the need for a comprehensive and society-wide approach to coping with emerging cyber risks.

According to the Swiss constitution, the Confederation has to safeguard Switzerland's independence and welfare. Related duties include assisting in the alleviation of need and poverty wherever they occur, and promoting respect for human rights, democracy, the peaceful coexistence of peoples, and the conservation of natural resources. I.e., while the principal interests of Swiss foreign policy are national independence, security and prosperity, preventing conflicts elsewhere fosters international stability, which in turn increases domestic security. The Swiss Foreign Policy Strategy for 2012 to 2015 defined four strategic axes, one of which addresses "continuing and adapting Switzerland's stability in Europe, in regions bordering Europe and in the rest of the world".

In 2016, Switzerland's Federal Council set out four strategic priorities in its Swiss Foreign Policy strategy for 2016-2019, one of which is "Peace and Security"[36]. This strategy's core objective is to "build on Switzerland's commitment to peace and security, lending significant impetus to a viable and just order"[37]. With this in mind, the Federal Council identifies, among other targets, "a peaceful, secure, and open cyberspace" as an area capable of positively shaping peace and security. Cyberspace, it advises, should rest on "clear rules and mutual trust"[38]. Against this backdrop, Switzerland's national cyber strategy recognises the importance of international cooperation to mitigate cyber risks. One measure in particular – measure 10 – states that "Switzerland cooperates at the international security policy level so as to counteract the threat in cyberspace together with other countries and international organizations. It monitors the respective developments at the diplomatic level and promotes political exchanges within the framework of international conferences and other diplomatic initiatives"[39].

The Swiss Contribution to the Development of the First Set of CBMs

Since the establishment of informal working group 1039, as required under the OSCE's mandate, Switzerland has been actively developing an initial catalogue of CBMs. One major Swiss contribution was the development of CBM number 7.

In improving the stability of cyberspace, Switzerland has emphasised the importance of the private sector. Partnering with the private actors is regarded as an appropriate means to tackle non-traditional threats to national security, such as cyberthreats. In fact, the national public-private partnership is acknowledged as a cornerstone of cyber risk mitigation. Considering that, in light of increasing privatisation, many OSCE delegations have similar arrangements with critical infrastructure operators, it is unsurprising that Switzerland was eager to introduce this concept into the OSCE framework.

35 | Federal Council, National strategy for the protection of Switzerland against cyber risks, 2012 (online) https://www.isb.admin.ch/isb/en/home/ikt-vorgaben/strategien-teilstrategien/sn002-nationale_strategie_schutz_schweiz_cyber-risiken_ncs.html (access 02.12.2015).
36 | Federal Council, Swiss Foreign Policy Strategy 2016-19: Federal Council report on the priorities for the 2016-19 legislative period, 2016 (online) https://www.eda.admin.ch/content/dam/eda/en/documents/publications/SchweizerischeAussenpolitik/Aussenpolitische-Strategie-160301_EN.pdf (access: 18.07.2016).
37 | Ibid p.21.
38 | Ibid p.25.
39 | Federal Council, National strategy for the protection of Switzerland against cyber risks, 2012, p.38. (online) https://www.isb.admin.ch/isb/en/home/ikt-vorgaben/strategien-teilstrategien/sn002-nationale_strategie_schutz_schweiz_cyber-risiken_ncs.html (access 02.12.2015).

The Swiss Chairmanship of the OSCE 2014: Combating Transnational Cyberthreats

In 2014, Switzerland assumed the OSCE Chair for the second time. As the first state ever to take on this challenging task twice, Switzerland signalled its willingness to help resolve conflicts via dialogue, constructive engagement and cooperation[40]. As an organization known for its inclusiveness, its constructive dialogue and its comprehensive approach to security, the OSCE provides an ideal platform to illustrate core values of Swiss foreign policy. Further, the broad toolkit of instruments at the OSCE's disposal, including CBMs and consensus-based decision-making, mirror similar features of Swiss foreign policy.

The leitmotif of the Swiss OSCE Chairmanship was "creating a security community for the benefit of everyone"[41]. With this in mind, Switzerland set its Chairmanship three priorities: promoting security and stability, improving people's living conditions, and strengthening the OSCE's capacity to act[42]. To implement these objectives, Switzerland formulated a set of priority action areas, one of which – defence against transnational threats – includes terrorism and cyber risks.

Following Russia's occupation of Crimea in early 2014, the Swiss OSCE Chairmanship coincided with the development of the ensuing crisis in Ukraine. The resulting geopolitical circumstances shifted the previously defined Swiss priorities into the background, making the resolution of the conflict between Ukraine and Russia the central Swiss objective. Still, even as Switzerland's Chairmanship was reshaped by this crisis, the cyber domain was one area where cooperation across political divides and divergent stances seemed possible.

40 | Federal Department of Foreign Affairs, The Swiss Chairmanship of the OSCE 2014: Final Report, 2015 (online) https://www.eda.admin.ch/content/dam/eda/en/documents/publications/InternationaleOrganisationen/osze/Beilage-01-Schlussbericht_EN.pdf (access 07.12.2015).
41 | Federal Department of Foreign Affairs, Swiss priorities during its chairmanship, 2014 (online) https://www.eda.admin.ch/eda/en/fdfa/foreign-policy/international-organizations/osce/die-schweiz-in-der-osze-troika/osce-chairmanship-2014/swiss-priorities.html (access 03.12.2015).
42 | Ibid.

Irrespective of an issue threatening to divide Europe, thereby severely diminishing cooperative security as a whole, the process on CBMs proved to be one where participating States remained willing to collaborate. Later the same year, despite the international climate of mistrust and uncertainty, the OSCE States managed to maintain their momentum, placing the first set of cyber-realm CBMs on the OSCE agenda.

"Even as Switzerland's Chairmanship was reshaped by this crisis, the cyber domain was one area where cooperation across political divides and divergent stances seemed possible.

Implementation of the first set of CBMs

Switzerland's role in promoting the implementation of the eleven CBMs was exemplary. Not only was it among the first group of states to hold comprehensive presentations on their national cybersecurity strategy and public-private partnerships, it also actively encouraged other delegations to share information. This constructive attitude contributed to the high level of information exchange. By the end of 2014, 13 states had delivered comprehensive presentations on their cyber policies, strategies and structures. Following this trend, a large number delivered similar presentations the following year. In 2015, as requested by Decision of the Permanent Council, about 40 participating States implemented one or more of the CBMs[43].

During the capital-expert meetings, the participating States seized the opportunity to outline their national cyber- and ICT security architectures. A significant number also shared and updated information and

43 | Coduri M., Speaker at Serbian OSCE Chairmanship in Office Event on Effective Strategies to Cyber/ICT Security Threats, Session I: Promoting the Implementation of the First Set of CBMs. Belgrade, 29 and 30 October 2015.

outlined their national and international activities for each of the agreed measures. In addition to contributing to this implementation process, Switzerland submitted a comprehensive consolidated overview of its national and international efforts and activities for each CBM. This not only illustrated the organizational structures, roles and responsibilities of the Swiss public entities dealing with cyber risks, but also delineated the Swiss approach to mitigating these risks, focusing on its decentralised, self-regulatory approach and non-mandatory reporting scheme.

> “ The implementation of CBM 9, which was designed to provide a glossary of cyber terminology, turned out to be very challenging, sparking a contentious debate.

The implementation of CBM 9, which was designed to provide a glossary of cyber terminology, turned out to be very challenging, sparking a contentious debate. First, terms such as “information security” signify different concepts in different states. In the proposed International Code of Conduct for Information Security, for example, the Russian Federation defined it as efforts to curb the “dissemination of information that incites terrorism, secessionism or extremism or that undermines other countries’ political, economic and social stability, as well as their spiritual and cultural environment”[44]. Naturally, as many states believe that this definition could be used to legitimise controls on freedom of expression, it is highly controversial. Second, many states find it difficult to define cyber and related terminology at any level, and thus lack even national-level cyber glossaries; and third, few delegations pushed for the development of a common glossary within the OSCE’s informal working group 1039.

Against these divergent viewpoints, Switzerland contributed to the implementation of CBM 9 via a research study. Conducted by the New America Foundation, this study’s objective was to compile existing terminologies and definitions in the cyber domain, then to clarify what the various states denote with each. Analysing publicly available information and documents (e.g., cybersecurity strategies) was considered a first stimulating step towards a better understanding of the differently signified concepts. The Swiss government commissioned this study primarily to support the implementation of CBM 9; however, in order to serve a much broader audience, encompassing policy makers, academia, the private sector, civil society and the media, the compilation was made public in a “Global Cyber Definitions Database”[45].

Discussion on a second set of CBMs

For the development of a second set of CBMs, Switzerland followed the call of US Ambassador Baer, the Chair of informal working group 1039, and submitted proposals for new measures. Again, Switzerland was among the first group of states to initiate negotiation on additional measures. At the core were cooperative measures designed to improve interstate relations. In collaboration with the German delegation, the Swiss developed six of the eighteen new measures suggested.

In parallel to the above-mentioned objectives, as holder of the 2014 OSCE Chair, Switzerland introduced a third track to advance the OSCE’s work in the cyber domain: an informal Chairperson-in-Office (CiO) event. While dedicated primarily to spurring holistic implementation of the first set of CBMs, this would also support the negotiation of a second set of CBMs. The conference took place on 7 November 2014.

Three main objectives were pursued[46]. First, to reduce the risks of conflict stemming from the use of ICTs and explore modalities that would further promote

44 | United Nations General Assembly, A/66/359, Developments in the field of information and telecommunications in the context of international security, 2011 (online) https://ccdcoe.org/sites/default/files/documents/UN-110912-CodeOfConduct_0.pdf (access 07.12.2015).

45 | New America Foundation, Global Cyber Definitions Database, 2014 (online) http://cyberdefinitions.newamerica.org/ (access: 24.11.2014).

46 | OSCE, Swiss Chairmanship in Office Event, Confidence building measures to enhance cybersecurity in focus at OSCE meeting in Vienna, 2014 (online) http://www.osce.org/cio/126475 (access 01.12.2015).

participation, the conference aimed to take stock of the implementation of the initial set of OSCE CBMs. Second, it supported the negotiation of a second set of CBMs, inter alia, by inviting presentations on CBMs implemented at the sub-regional level and within other regional contexts. Third, it provided a platform for non-governmental stakeholders, e.g., providers of critical infrastructure, allowing them to express their needs and expectations regarding the OSCE CBM process.

For the first time, a state-centric multilateral process was broadened and opened up to non-governmental actors. By inviting an outside view, Switzerland aimed to learn from other stakeholders' and regions' experiences. A total of 130 private sector cybersecurity experts, think tanks, and representatives of civil society and academia from roughly 50 OSCE member and partner countries convened in Vienna to discuss possible improvements to the OSCE process on CBMs[47]. Through this event, by involving other than state actors, Switzerland accommodated the multifaceted interdisciplinary character of the matter at hand. As Ambassador Benno Laggner, former Head of the Division for Security Policy at the Swiss Federal Department of Foreign Affairs and Head of the Swiss delegation, put it, "governments and policy makers cannot go it alone. The involvement of technical experts, social scientists, policymakers and civil society is needed"[48]. Acknowledging the OSCE spirit of cooperative security, he added that "mutual understanding and trust can be achieved "by means of dialogue, engagement and commitment"[49].

The Swiss OSCE Chairmanship released nine recommendations on the development and implementation of CBMs[50]. These helped develop the Swiss priorities and the Swiss OSCE agenda for the coming years. Considering the outcome of the CiO event, Switzerland decided to focus on the following three issues:

1. **Dual-focus approach:** continuing with the implementation of the first set of CBMs while concurrently developing additional measures to build confidence.

2. **Cross-fertilisation:** improving inter-regional exchanges and linking the tasks conducted via the various fora. This goal also included the promotion of the instrument of CBMs as a means to prevent conflict. Thus, Switzerland strived to globalise CBMs.

3. **Outreach:** reaching out to other stakeholders, involving the private sector, academia and civil society to systematically improve security surrounding not only ICT, but also the entire OSCE process.

Conclusion and Recommendations

Recent events at the global and regional level have positively shaped international normative development in the cyber domain. Building interstate confidence through systematic dialogue, commitment and cooperation is an exemplary strategy to devise a normative framework in the cyber realm. The OSCE's groundbreaking process on CBMs in this domain makes it the first regional security organization to codify a set of measures to build confidence via transparency, cooperation and stability. Designed to reduce the risk of conflict stemming from ICT use while reducing the risk of misperception and miscalculation, the OSCE has made strong progress in the service of international peace and stability.

47 | Ibid.

48 | Laggner B., Speaker at the Swiss OSCE Chairmanship-in-Office-Event "Information and Communication Tech-nologies (ICTs) and Confidence Building Measures (CBMs): Promoting implementation, supporting negotia-tions, CIO.GAL/238/14, Vienna, 7 November 2014. (online) http://www.giplatform.org/sites/default/files/Summary%20Chairmanship%20in%20Office%20Event.pdf (ac-cess 06.12.2015).

49 | Op. cit. OSCE, Swiss Chairmanship in Office Event, 2014.

50 | OSCE, Swiss Chairmanship in Office Event, OSCE Chairmanship Event Summary, Information and Communi-cation Technologies (ICT) Confidence Building Measures (CBMs): Promoting implementation, supporting negotiations. CIO.GAL/238/14, 22 December 2014, OSCE+ (online) http://www.giplatform.org/sites/default/files/Summary%20Chairmanship%20in%20Office%20Event.pdf (ac-cess: 05.12.2015).

> Building interstate confidence through systematic dialogue, commitment and cooperation is an exemplary strategy to devise a normative framework in the cyber realm.

Switzerland has actively supported the OSCE process on building confidence in cyberspace, using the regional security organization as a multilateral venue to promote the peaceful use of ICTs. Linking the goals outlined in the Swiss constitution and refined in the Federal Council's Swiss Foreign Policy with the national strategy for Switzerland's protection against cyber risks, it becomes clear that cybersecurity is not only a precondition to international peace and stability, but a catalyst for prosperity and human rights. The obverse is also true: its absence has a destabilising effect on international peace and stability.

In line with the OSCE's acquis, Switzerland has been committed to resolving conflicts through inclusive dialogue, enduring engagement and cooperation. As Switzerland vigorously pursues its security and foreign policy interests in cyberspace, like the OSCE, its comprehensive approach to security employs a broad array of instruments designed to prevent and manage conflicts. A further commonality is its consensus-based approach, which allows consideration of a plurality of views and standpoints.

Switzerland has proactively engaged in the development of CBMs and supported the OSCE process since its inception. Not only did it support implementation of the list CBMs, but it also encouraged other delegations to participate in the information exchange. In fact, the Swiss delegation's proactive behavior and outreach towards other participating States has contributed to the establishment of an environment that supports and encourages coherent and systematic dialogue. In addition, Switzerland has helped initiate a debate on measures designed to strengthen inter-state cooperation. With other OSCE member States, Switzerland also contributed to the adoption of additional CBMs in March 2016. The organization of a Chairmanship in Office Event – which has developed into a permanent feature in the OSCE process – led to a series of recommendations as to how participating States can improve the work of informal working group 1039.

Against this backdrop, Switzerland can be regarded as a driving force for the OSCE confidence-building process: Swiss activities have imparted it with visibility, both within and beyond the OSCE region. The Swiss have also promoted CBMs as a reliable means to prevent conflict. Further, Switzerland has proactively reached out both to OSCE partners and to non-state actors as stakeholders in an otherwise state-centric process. Among its achievements, Swiss engagement has led to recurrent expert roundtables and panels representing academic experts and civil society.

> At the levels of foreign policy and international engagement, Switzerland is a latecomer, with its national cyber strategy giving it the mandate, and thus the legitimacy to debate on an international stage.

Conversely, the OSCE process on CBMs has helped Switzerland define and develop its security and foreign policy profile in the cyber domain. In 2012, the adoption of the Swiss national cybersecurity strategy coincided with the establishment of informal working group 1039. Until then, Switzerland's cybersecurity structural and organizational posture was limited to the technical-operational level, focusing mainly on responding to incidents. At the levels of foreign policy and international engagement, Switzerland is a latecomer, with its national cyber strategy giving it the mandate, and thus the legitimacy to debate on an international stage. An ideal venue, the OSCE constitutes the first multilateral framework within which Switzerland has advanced its cyber-related

interests. In fact, Switzerland's stance in the cyber domain grew by means of and thanks to the OSCE.

Thus, the OSCE has become one of the most influential multilateral processes to advance security and stability in cyberspace. With this in mind, Switzerland is well advised to maintain active engagement for the foreseeable future. To this end, the author suggests a small number of recommendations.

First, it should be recognised that Switzerland is one of the world's leading countries in the use of ICTs. An export-oriented state benefiting fully from the Internet commerce, its current and future viability depends on an open, free and secure cyberspace[51]. Not only do cyber attacks pose risks to citizens, companies, and states, but they also undermine confidence in the cyber domain as a whole. Likewise, any attempt to subject cyberspace to increased state control or otherwise advance states' interests in this domain can destabilise and fragment this infrastructure. This would diametrically oppose Switzerland's interests. Therefore, Switzerland has a strong incentive to shape the global cyber environment and contribute to the development of rules governing state behaviour in cyberspace.

Second, considering the success of the dual-focus approach to CBMs, the OSCE's informal work group 1039 should continue to implement the full set, while dedicating time to further developing more. However, the participating States should continue to improve the implementation process. Even with the majority of participating States engaged, almost a third of delegations have not yet used this forum to exchange information, let alone implemented the first set of CBMs at national level. Identifying why certain participating States have refrained from contributing to CBM implementation should be a priority for Switzerland. If the lack of participation results from organizational and institutional gaps, Switzerland could help bridge them. If, however, certain delegations fail to see how participating in the process will further their national interests, Switzerland could be decisive in convincing them of the value and utility of OSCE participation.

The third recommendation is linked to the second. Implementation needs to be meaningful. While implementation to date can be regarded as a positive beginning, it is clear that participating States' endeavors need to progress beyond mere information exchange. Members need to strive for a more standardised mechanism to target and inform other delegations.

Fourth, implementation needs to be reviewed on a regular basis. Citing the voluntary nature of OSCE participation, informal work group 1039 has refused to define certain modalities that would implement the full set of CBMs. This has resulted in a certain level of imbalance. While certain CBMs have been implemented across almost all participating States (e.g. CBM 7), others have not yet been implemented anywhere (e.g. CBM 3). Review and verification of the implementation process could be an area upon which the OSCE delegations would agree. One way of moving in this direction would be creating sub-groups to evaluate the implementation process. Being a neutral and credible actor, Switzerland could chair one of those and provide recommendations as to how participating States can engage more strategically and more effectively in OSCE work.

Fifth, the voices of civil society, the private sector and academia need to be amplified in the OSCE context. Given these actors' vital roles regarding cyberspace security and stability, Switzerland could use its inclusive traditions to involve them.

Sixth, the complex challenges arising from the dynamic and rapid development of cyberspace demand specific expertise and knowledge. While technological capabilities are moving at lightning speed, related policy and legal frameworks are lagging. Sharpening the diplomatic community's awareness of this situation could be an area of stronger Swiss engagement. For example, Switzerland could employ existing platforms, such as the Geneva Internet Platform, to pool and share knowledge that would increase policymakers' understanding.

51 | Op. cit. Burkhalter, 2015.

These recommendations are based on the premise that, while the OSCE provides a workplace where all participants can work together to develop, shape and benefit from its confidence-building measures, the ultimate success of those measures, and of the OSCE itself, depends on their overall acceptance and use. Switzerland is well positioned to promote that outcome. As participation and cooperation regarding cybersecurity within the OSCE arguably further Switzerland's commitment to international peace and stability, this article concludes that the OSCE is a critical regional organization fostering security through multilateral channels. What is more, the authors argue that, for Switzerland, the OSCE process on confidence-building measures in cyberspace has been instrumental in developing its foreign policy profile and defining its international posture in the cyber domain. ■


Security for the cognitive era.
When everything is connected, everything is vulnerable. IBM uses cognitive technology to help protect the critical assets of your business. It senses and helps detect millions of hidden threats from millions of sources, and continuously learns how to defeat them. When your business thinks, you can outthink.
outthink threats
IBM and its logo and ibm.com are trademarks of International Business Machines Corp., registered in many jurisdictions worldwide. See current list at ibm.com/trademark. Other product and service names might be trademarks of IBM or other companies. © International Business Machines Corp. 2016.
ibm.com/outthink

INTERVIEW WITH ALASTAIR TEARE

ALASTAIR TEARE
currently serves as CEO of Deloitte Central Europe, a position he has held since 2012. Alastair has been with Deloitte his entire career, having begun in their London office in 1990 before being seconded to Budapest in 1993.

Since becoming a Partner in Deloitte Central Europe in 1999, Alastair has held many roles, including Partner in Charge of Audit in Hungary, Regional Reputation & Risk Leader, a member of the Deloitte CE Board of Directors and a member of the Deloitte CE Executive Committee. He is also a member of the Deloitte Touch Tohmatsu Limited (DTTL) Board of Directors.

With over 26 years of experience in professional services, Alastair has had the opportunity to serve a diverse portfolio of clients, mainly leading teams to deliver assurance and advisory services to large financial institutions in Central Europe.

Alastair strongly believes in building a unique experience that attracts the best talent, builds on their own strengths and inspires them to deliver outstanding value to clients and he is a strong proponent of the Deloitte Purpose: To make an impact that matters for their people, their clients and society.

The decision where to locate a cyber-related business depends on a number of factors; the available skills and competences are a key determinant among these. Is talent really the most crucial resource while talking about cybersecurity? Is technology not enough to solve IT-related issues?

The need for cybersecurity is increasing rapidly as cyberthreats become more frequent and more sophisticated. To make a change in this area requires more time and effort than simply buying and implementing technology. There is no doubt that skilled and trained people are the most crucial factor in counteracting these threats. The important question is where these people will come from and how we can attract them.

Deloitte organises special training programmes in order to find the right candidates for its team of cybersecurity consulting experts. Could you tell us more about the specific qualifications Deloitte is trying to develop?

We do have specific programmes that we are developing in our dedicated cyber teams and we have created a series of bespoke exercises we call “Capture the Flag”, used to assess and build on the skills of potential recruits. Capture the Flag is a training game where participants face off with virtual computer systems. We monitor each person in detail, evaluating their responsiveness and awareness as well as their levels of identification and exploitation. This is a fun way to test skills in infrastructure and application so that we can build up and train where required. We also have a robust training curriculum for new joiners. After that, it’s a long journey to get on track. The complexity of cyberthreats evolves rapidly and so does our curriculum. Training continues to escalate throughout our employees’ career journey with Deloitte, ensuring the qualifications and skills of our people are up to date so that our teams can grow and adapt to the changing cyber landscape.

We have learnt about Deloitte's strategy. Now, how do you intend to overcome the talent shortage that can be observed globally within the technology sector?

We have a truly distinctive talent experience at Deloitte. Many of our people come to us for the opportunity to work with interesting clients, to test and work with new systems and to experience new challenges every day. Yes, the competition for talent is very high, but I believe that by being a purpose-led organisation striving to make an impact that matters, we offer the chance for our people to build on their own skills and interests, empowering them to achieve more than they could elsewhere.

During the European Cybersecurity Forum CYBERSEC in Kraków, you said that team efforts coming from various stakeholders are needed to build conditions that may boost innovation in the area of cybersecurity. How to achieve this goal? How to overcome rivalry tendencies between actors in order to jointly upgrade the overall cybersecurity ecosystem?

We can't make people innovative, but we can build a culture of innovation where we continuously expose our people to new experiences and new ideas. By creating our own internal incubator for creativity and knowledge sharing, we are able to expose our people to as many areas of our strategy as possible. There is a need for governments to take a lead in this area and to encourage research and development activities, which would be best performed by universities and research institutes working closely in partnership with the private sector to create a common platform from which to address mutually agreed goals.

In one of the most recent Deloitte reports, we learn that as the competitive landscape continues to grow, organisations that fail to develop a robust cybersecurity position may struggle to defend their critical data assets more than their business rivals. Could you please point out a few top factors of success that you would mention to your clients when advising them on cybersecurity experts team building?

To be a cybersecurity expert, we recognise that the skill-set requires deep expertise and a different mindset. We are looking for inquisitive thinkers who can work around problems and explore solutions in a non-linear way. That said, we also recognise that our target group are looking for an exciting experience and work that will challenge them. We do provide these challenges, not only through real-life client interaction, but also through training exercises. On top of that, we provide an atmosphere where there is room to constantly grow and learn. All of these diverse factors must come together to attract the right people, and I think that's exactly where Deloitte has the edge on our competitors. ■

Questions by:
Dr Joanna Świątkowska
The Kosciuszko Institute

ANALYSIS

ADVANCING SECURITY MONITORING OPERATIONS

BRETT TAYLOR
is the Cyber Pre-Sales Technical Manager in the International Services & Solutions Divisions at BAE Systems Applied Intelligence. As such, he is responsible for redefining the way BAE Applied Intelligence delivers cyber capability to the market internationally. He has over 20 years of experience in IT/OT management for OSS, Cybersecurity and Law Enforcement/Intelligence and is a regular conference speaker on those subjects. He held leadership posts in large systems integrators (IBM/Cap Gemini), defence contractors (Boeing/BAE) and network equipment providers (Alcatel Lucent).

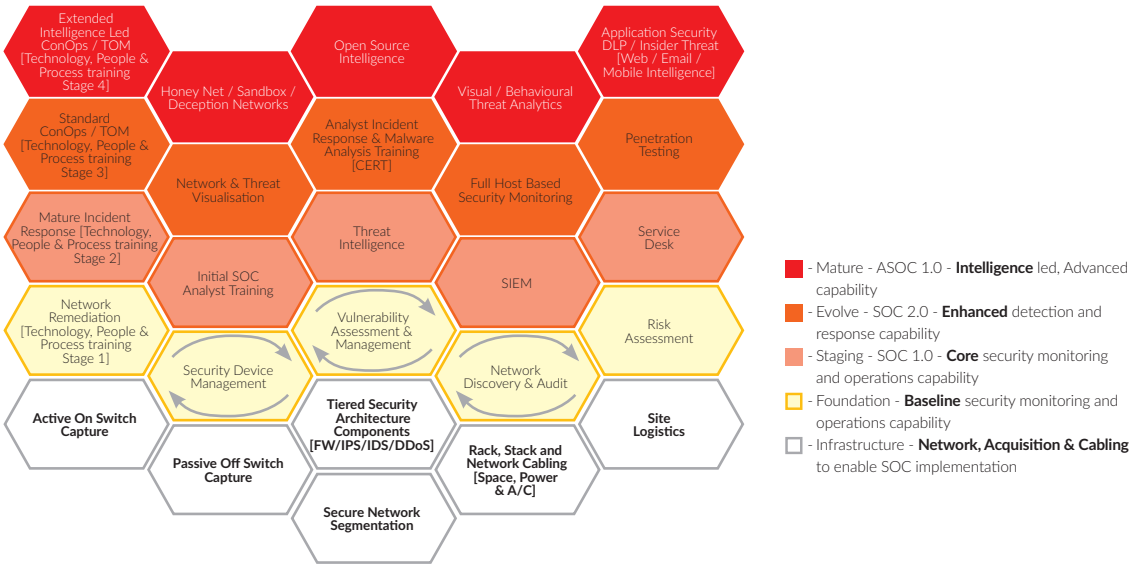
Moving from reactive tactical firefighting to proactive strategic defence

Designing and delivering large-scale programmes for network monitoring, cybersecurity and communications intelligence both nationally and internationally is a complex technology problem that should never be approached with a big-bang methodology. It should be broken down into manageable components that deliver capability along a phased programme trajectory, all the while building towards a realistic and achievable set of goals. These goals realise the host organisation's aims, and exceed them through the delivery approach and rigour of the implementing organisation and its people.

One such problem that benefits from this approach is the proposition of an Advanced Security Operating Centre [ASOC] – a facility that takes the reactive monitoring function traditionally seen in this domain and turbo charges this model with intelligence-led technologies, processes and people. By doing so, it transforms the traditional SOC operations from a bottom-up, network-focussed view, and enables a top-down, intelligence-led ASOC approach to cyberdefence – providing greater visibility of the threat actors, their tools, techniques and vectors of attack as well as a wider view of the attack fabric.

BAE Systems Applied Intelligence has developed an ASOC model that is a blend of multiple complementary technologies, integrated to provide a hardened cyber perimeter, where the sum of the parts is greater than their capabilities deployed in isolation. Naturally, this kind of integrated offering is complex, as the technology needs to evolve in step with the processes and the capabilities of the people who will ultimately staff and run the facility.

Figure 1. BAE Systems AI Complete ASOC Model



The security architecture of the ASOC model is designed to be open, modular and flexible, allowing customers to engage, either from a greenfield site or a position where investment has already been made in technology. This approach enables replacing tools over time as they are superseded, as well as extending the model horizontally and vertically as new or deeper capabilities are identified, without disrupting the core operations of the facility.

The following sections detail the phased tiers of the ASOC model security architecture, and the intent behind each tier's implementation.

As can be seen in Figure 1, the ASOC model is comprised of 5 tiers of capability. These tiers are described in further detail below:

Infrastructure

This tier of the ASOC model is comprised of six elements, which provide the following capabilities:

Site Logistics – Provides recommendations that focus on ensuring that the site[s] chosen for the ASOC platform are adequately provisioned in terms of site facilities, physical security, safety and accessibility.

Rack, Stack & Network Cabling – Implementation of recommendations for the application equipment hosting the ASOC components. Typically, a rack layout is provided, alongside specifications for servers, and the way they are to be cabled to support the enterprise and enable proper ASOC communications.

Additionally, power and cooling requirements will be provided to ensure that all equipment can operate within the defined limits of the associated warranties.

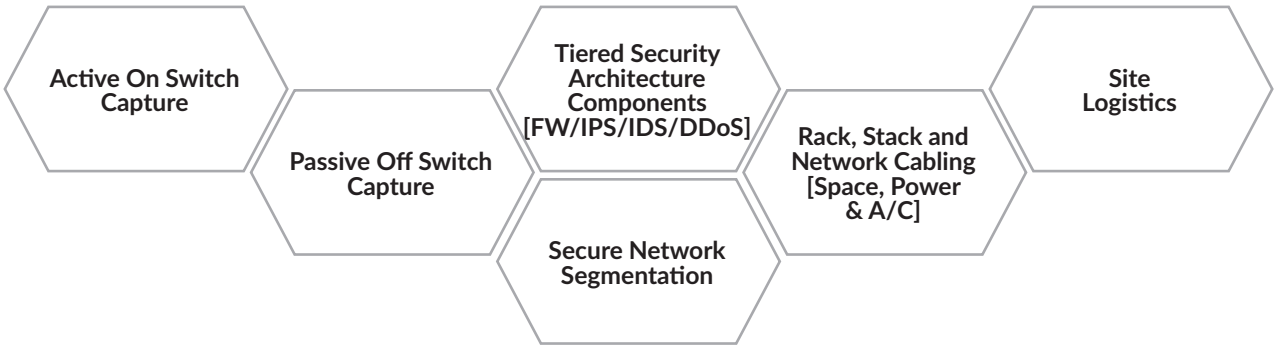
Tiered Security Architecture Components – Implementation of recommendations that focus on the tiered security architecture of the enterprise, identifying weaknesses and correcting them. The purpose of this activity is to ensure that the hardware which protects the ASOC application infrastructure is fit for that task

Secure Network Segmentation – Using specialist equipment to monitor the directionality/flow of network information between LAN segments. This technique makes it harder for malware to proliferate across segments, by designing the expected traffic that the segment will see as a profile, and applying that profile uni- or bi-directionally at the segment boundary.

Network Sensor Hardware – These are deployed to capture communications meta-data and/or content passively within the enterprise boundary.

Network Sensor Software – These are deployed to capture communications meta-data and/or content actively within the enterprise boundary.

Figure 2. ASOC Model: Infrastructure Tier



Foundation

This tier of the ASOC model is comprised of five elements. The intent is for this tier to provide a secure hardened network platform, protected from all known threats, upon which to build the ASOC solution components as follows:

Risk Assessment – This is a consultancy activity looking at the 'as-is' state of the enterprise network [technology, people & process] and building a plan of activity and recommendations for both the infrastructure and tools to enable the 'to-be' model successfully.

Network Discovery & Audit – This activity enables a complete network discovery so that an accurate snapshot of devices and their configurations are captured for analysis of potential problems. This process runs iteratively over time to ensure that the enterprise topology understanding remains accurate as it grows or shrinks.

This iterative discovery forms the baseline against which vulnerability and security device management functions will integrate and run.

Vulnerability Assessment & Management – This function is tightly integrated with the network discovery technology. A fingerprint of the discovered network is built, against which a large store of known vulnerability signatures is run, escalating to the ASOC analysts when one is found for remediation.

This approach drastically decreases the time between vulnerability discovery and remedial action, so malware has a reduced window of opportunity to execute its mission.

Security Device Management – This addresses elements of the enterprise architecture that provide security-related functions, such as a firewall or intrusion detection/prevention system [IDS/IPS]. It looks for device configuration errors, access credential problems & old running firmware/software that should be patched.

Network Remediation – This element comprises some standard cyber concepts training, coupled with specific tools training and the processes required to operationalise the SOC. It enables a customer to administer and use the products themselves for the protection of the underlying application infrastructure, after the initial systems have been implemented.

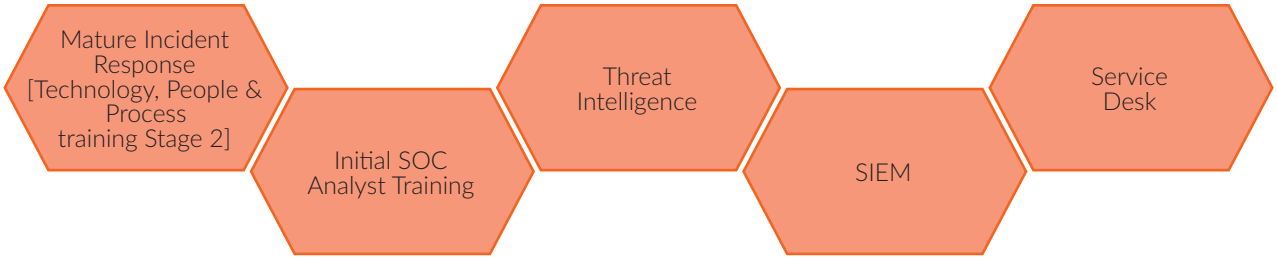
Staging

This tier of the ASOC model is comprised of five elements. The intent is to provide ASOC service management, security event aggregation and correlation, and threat horizon scanning and policy, the details of which are discussed further in the sections below:

Service Desk [SD] – This component manages all issues relating to the operational running of the ASOC service on the customer's enterprise, providing tools for escalation, triage and remediation of faults and security incidents, with full audit capabilities, service reporting and measurement.

Figure 3. ASOC Model: Foundation Tier

Figure 4. ASOC Model: Staging Tier



Security Incident and Event Management [SIEM] – This component aggregates security event data received from multiple sources, and then normalises and correlates the data to present it as a stream of rich security intelligence against which analysts can act and enforce an appropriate remedial policy.

Threat Intelligence [TI] – This capability is provided as a management technology alongside a subscription service. This enables customers to ingest and utilise sources of intelligence that describe attack group methodologies or infrastructure. From these intelligence sources, all key elements can be extracted [IP addresses, email addresses, domains, URLs etc.], providing a means to generate policy configuration rules, which can be pushed down to the components in the tiered security architecture.

Through this approach, customers can determine the threats observed in their region and take proactive steps to upgrade their security perimeter based upon that analysis, essentially operationalising the received threat intelligence.

Initial SOC Analyst Training – This is an element of the BAE Systems Cyber Academy programme, empowering users with the operational processes and technology training to run the ASOC effectively. It maps these processes and training to the SIEM, TI and SD products, and forms the foundation of the full process model required to achieve a proactive intelligence led capability.

Mature Incident Response Training – This training activity builds on the earlier Network Remediation component at the Foundation stage of the model, enabling appropriately skilled customer resources to act on tickets raised through the Service Desk and remediate security incidents/faults in the enterprise network.

Evolve

This tier of the ASOC model is comprised of five elements. The intent of this tier is to provide proactive testing and reverse engineering capabilities, alongside host-based monitoring and visualisation of the threat vector path[s] through the enterprise network, discussed further in the following sections:

Penetration Testing – This activity is a proven way to identify and fix vulnerabilities that exist in a network proactively before threat actors can leverage those deficiencies. This testing in the ASOC context uses a broad range of attack methods, conducted initially by BAE Systems security specialists, and later by customer staff as they become proficient in the methodology. The attack techniques used are essentially the same as those a hacker or another threat actor would use, and so the activity exercises the defence posture of the enterprise and forewarns it if that cyber perimeter is porous.

Full Host-Based Security Monitoring – Host or end-point security is essential to the continued health of the ASOC and the users of the enterprise network that it protects. This component locks down end-points and critical host systems. It arms the ASOC incident response team with advanced tools to hunt down host-based threats, ranging from file-based malware and ransomware attacks to memory-based, power shell, script-based or obfuscated malware vectors.

Figure 5. ASOC Model: Evolve Tier

This security posture is achieved through a full spectrum analysis approach, encompassing behavioural, reputational, signature, AI and machine learning techniques.

Malware Analysis Training – This element of the ASOC model provides a deeper understanding and training in the tools and techniques used to deconstruct identified malware, and to enhance from that analysis the deployed components of the ASOC in order to harden the cyber perimeter against future attacks of the same or similar type.

This is an advanced component requiring specific skills, such as reverse engineering of compiled executables, examining how malware interacts with the host environment, understanding propagation characteristics and definition of signatures.

Network & Threat Visualisation – This component exposes a blended view of threat vector path, overlaid on the discovered network footprint [both physical and logical]. This enables the ASOC analysts to quickly and intuitively identify breaches, and more importantly, their impact – directing an appropriate response in a timely manner and tracing the threat back along its infection path to the source of the breach.

Standard ConOps / TOM – As each tier of the ASOC delivery is realised, it is important to ensure that the right processes are matured alongside the technology and people. This element is the third iteration of this deliverable, further maturing the process model to the full standard ASOC Target Operating Model [TOM] and associated Concept of Operations [ConOps].

These documents are tailored to the receiving organisation and allow new starters to understand the operational blueprint for the ASOC and deliver operational benefit more quickly.

Mature

This tier of the ASOC model is comprised of five elements. The intent of this tier is to provide intuitive visual and behavioural analytics, fused data sources, application intelligence and malware sandboxing alongside an extended TOM/ConOps for intelligence-led operations. These capabilities will be further detailed in the sections below:

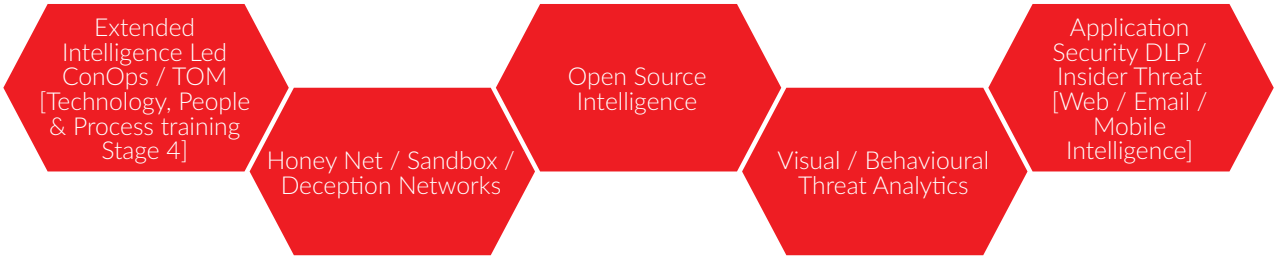
Application Intelligence – Focusing on the critical applications running on the enterprise network, and how best to secure those applications and users. This is achieved through several disciplines:

Mobile Device Management [MDM] – Protects classified company data and communications on mobile devices to enable policy compliance and network security.

Targeted Attack Protection [TAP] – This technique significantly reduces security exposure for the enterprise network, protecting from reputational damage and intellectual property theft from cyberthreats with fast and effective attack detection, containment, and response.

Email Protection – Comprehensive capability in the following key domains: Email Security, Email DLP, Email Encryption, Email Archive and Email Continuity.

Figure 6. ASOC Model: Mature Tier



Threat Analytics – This component can store, process and rapidly query billions of infrastructure events per day and do so cost-effectively on commodity hardware. It provides an abstraction layer at the ingress of data, allowing the platform to be agnostic to the specific data source and format being ingested. All data is normalised into standardised formats, which can later be used at the analytics stage of the solution.

Once the data has been ingested, it is stored with granular, cell-level security as normalised key/value pairs. This enables queries that can retrieve a subset of events from the whole dataset in a matter of seconds.

Once indexed, analytics can be run across the entire breadth of the data stored, identifying traditional as well as new attack methods and zero-day exploits, as well as enabling analysts to write their own analytics using the same toolset.

Open Source Intelligence – This provides an interactive tool to enable analysts to investigate open source material from multiple viewpoints and internet sources, quickly visualise people, locations, topics, links and other data. Data collection is typically based upon providing keywords and / or geographic locations against a set of sites, or collecting from entire sites (e.g. forums).

Data is processed using a big data pipeline in which data is enriched using best-of-breed components, such as sentiment analysis, language ID / processing, entity extraction, EXIF extraction, theme analysis and more. The information is then stored in a big data index and presented in near real-time for visualisation and analysis using the ASOC toolset.

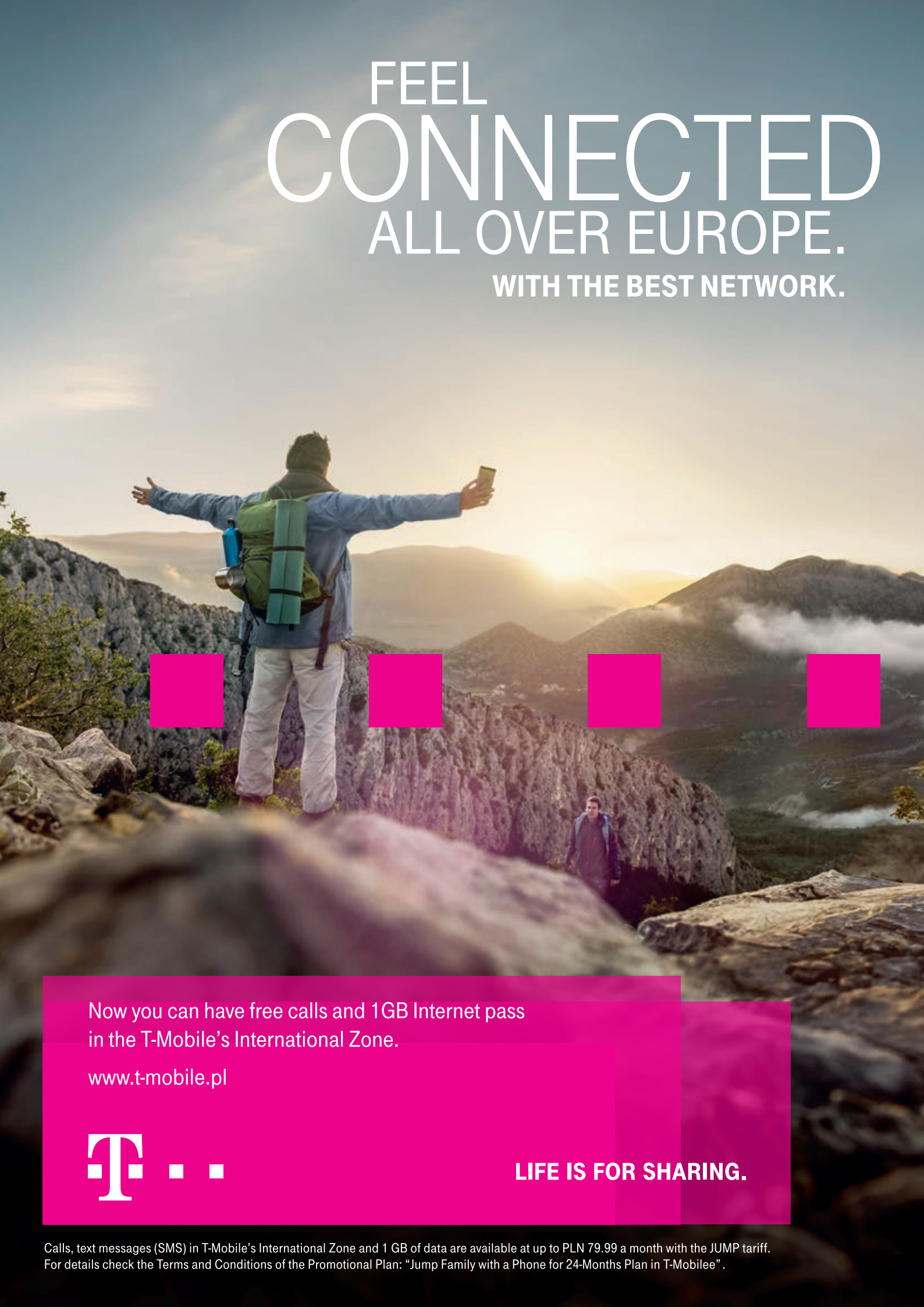
Deception/Honey Networks – This tool provides a distributed deception and decoy solution that is designed to detect, deceive and defend against multiple cyberthreat vectors.

It does so by instancing a deception network infrastructure that any attacker must traverse before hitting the live cyber perimeter, allowing the observation of attacks in a non-reactive state, identification of lateral movement, and use of baits, lures and decoy services to facilitate exposure of attack techniques.

Extended Process Model for Intelligence-Led Operations – The final tier of the ASOC model introduces sophisticated technology components and extends the process and technical capability of the ASOC. This naturally requires an evolution of the standard process model and people training elements to meet this proactive intelligence-led approach.

Summary

To deliver strong in-depth cyberdefence using an integrated software approach is a complex undertaking. What I have detailed in this article is one approach to achieve this goal, and an approach that has been successfully used on a national scale. Only by using these methods will we be able to catch up, keep up and evolve our defences to meet today's, but more importantly, tomorrow's cyberdefence needs. ■



Calls, text messages (SMS) in T-Mobile's International Zone and 1 GB of data are available at up to PLN 79.99 a month with the JUMP tariff. For details check the Terms and Conditions of the Promotional Plan: "Jump Family with a Phone for 24-Months Plan in T-Mobilee" .

ANALYSIS

MAPPING OUT ONLINE JIHADISM: A CASE STUDY OF TWITTER AND TELEGRAM

PEPIJN BIERHUIZEN
is a University of Amsterdam graduate with a New Media and Digital Culture BA and MA, and a minor in Intelligence Studies. He is currently in training to become an officer in the armed forces of the Netherlands.

Extremist groups are able to radicalize sympathizers and inspire them to join their cause through the use of social media. It is, therefore, vital to understand the way they are weaponizing social media and mapping out their online networks in full in order to monitor their activities and implement successful and lasting countermeasures. While the focus of this article is on the Islamic State (ISIS), who is notorious for its effective and wide-scale weaponization of social media, it is unlikely to be the last group to do so. It is, therefore, essential to develop methods for monitoring such groups online.

By doing empirical research, I investigated the possibility of using the affordances of Twitter, a microblogging platform and Telegram, an encrypted messenger service, to map out the use of these platforms in ISIS' online information dissemination network. This was done by collecting tweets containing both Arabic and English hashtags used by ISIS as well as messages in several Jihadi Telegram channels. The subsequent analysis showed the centrality of these two platforms in the network, and a strong interconnectedness between these and other platforms. Chiefly, the results of the analysis hint at resilience built into the network itself, which is essential to its survival in the face of censorship.

1. Introduction

"The wide-scale spread of Jihadist ideology, especially on the Internet, and the tremendous number of young people who frequent the Jihadist websites, [are] a major achievement for Jihad." – Osama bin Laden, 2010[1].

Platforms like Twitter and Telegram are used to attract new recruits by propagating the message of Jihad: a holy war against the enemies of Islam. Besides being utilised to radicalize individuals and for fundraising, tools such as Telegram are also exploited to coordinate attacks as was the case with the November 2015 Paris attacks, killing 130 and leaving hundreds wounded[2]. While Telegram removed Jihadi channels and users after the news broke it had been used during the attacks, little has been done since. Twitter has increased the vigour with which they fight Jihadis , but this has by no means eliminated Jihadis[3] from the platform.

On Twitter, hashtags are the only central element in a distributed network. Here Jihadi content is shared by many different accounts via tweets containing hashtags and hyperlinks to content-hosting platforms.

> "Extremist groups are able to radicalize sympathizers and inspire them to join their cause through the use of social media.

While the Jihadi accounts and content are both subject to censorship elsewhere, on Twitter hashtags are not, and thus make Jihadi material and accounts easily findable. Using hashtags as a starting point, it is possible

1 | Qtd. in Stalinsky S. and Sosnow R., From Al-Qaeda To The Islamic State (ISIS), Jihadi Groups Engage in Cyber Jihad: Beginning With 1980s Promotion Of Use Of 'Electronic Technologies' Up To Today's Embrace Of Social Media To Attract A New Jihadi Generation, MEMRI Jihad and Terrorism Monitor, 2014, p.25.
2 | Billington J., Paris terrorists used WhatsApp and Telegram to plot attacks according to investigators, International Business Times, 2015.
3 | Yadron D., Twitter deletes 125,000 Isis accounts and expands anti-terror teams, The Guardian, 2016.

to map out an important part of the Jihadi dissemination network.

While there is no centralizing element in Telegram, messages in Telegram channels and groups provide avenues for a more in-depth look at how the application is being used to share content and links to other Telegram channels and Twitter accounts.

This article falls in the field of Internet Research, specifically in the sub-fields of Open Source and Social Media Intelligence (OSINT/SOCMINT). In these fields, the Internet is used as a tool for and a method of doing research to map out actors and practices. This paper aims to contribute by providing a hashtag-based approach on Twitter and an object-based approach on Telegram, and reflecting on using such digital methods to do intelligence research. The countermeasures taken to evade censorship and preserve an online presence can only be overcome by delivering a crippling blow to the network as a whole instead of targeting individual platforms. Like the Internet itself, E-Jihadism was built to route around damage. Only when as many connections as possible are severed simultaneously do the possibilities for reconnecting cease to exist. Fighting a distributed network requires a distributed approach.

2. E-Jihadism

During the 1990s, Jihadism went online with the launch of the first Jihadi websites and forums. Over the course of a decade, Jihadi Internet forums became the most prominent place for E-Jihadism, and later, during the 2010s, social media were weaponized by various Jihadist groups and individuals. The increasing importance of social media was due to the fact that they offered more room for discussion than the forums which were subject to strict censorship by moderators. Furthermore, more potential sympathisers could be reached and links to content on other platforms could be disseminated more easily[4]. While contemporary E-Jihadism relies on many platforms, Twitter was the most important platform up until the end of 2015. It was during that time when Twitter increasingly censored Jihadis using the platform, forcing them to adopt alternative media such as Telegram. With Telegram, Jihadis could easily disseminate content without having to worry much about censorship.

Before official content can be shared on Twitter, Telegram, or on any other platform used by Jihadis, it has to be produced. This is done inside the occupied territories by media outlets such as ISIS' Al-Hayat Media Center[5], distribution offices such as Nashir, or its news arm – Amaq Agency[6]. When content such as a video has been shot and edited, it is uploaded to hosting platforms, after which the link to the content is disseminated on social media. Uploads are often accompanied by a specific hashtag such as the name of the associated media outlet[7], or the title of the video. The content can be downloaded by sympathisers, many of whom then proceed to upload and share the content themselves[8]. The use of hashtags and the industrious uploading of content means that it is relatively easy to find a working link on a number of different platforms.

The organizational structure of contemporary E-Jihadism has been described as a swarmcast: a distributed network that is able to disperse and reassemble quickly in a chaotic environment that is subject to censorship[9]. With little centralized or decentralized coordination, the swarmcast relies on a distributed power architecture. Ayman al-Zawahiri, the successor of Osama bin Laden, spearheaded this approach by urging Jihadis not to tie themselves to any organization, leader, or territory. Instead, they should embrace Jihad individually[10]. This works especially well online. Jihadis expect censorship and have thus prepared for it by creating multiple accounts on multiple platforms, so that if an account or

4 | Zelin A.Y., The State of Global Jihad Online: A Qualitive, Quantitative, and Cross-Lingual Analysis, New America Foundation, 2013, p.4-5.

5 | Ibid p.6.

6 | Benjamin S., Understanding The ISIS Media Apparatus: Distribution Networks And Practices, Jihad and Terrorism Threat Monitor, 2016.

7 | Some of the analyzed hashtags in this article correspond with the above mentioned outlets.

8 | Op. cit. Zelin 2013, p.6.; op. cit. Benjamin 2016.

9 | Bartlett J., and Fisher A., How to beat the media mujahideen, "Demos Quarterly", February 2015.

10 | Fisher A., Swarmcast: How Jihadist Networks Maintain a Persistent Online Presence, "Perspectives on Terrorism", 2015, p.6.

a platform becomes unusable, they can quickly shift to another, placing or linking to content there. Substitute networks are already present or can be formed quickly by spreading the word on other platforms, where a network is already formed, on what new platforms and accounts to join or follow. This multiplatform approach is crucial to the survival of E-Jihadism[11].

> "The embrace of E-Jihad is a successful attempt to both spread the Jihadist ideology as well as to weaponize sympathisers without making them cross physical and moral boundaries they might not be prepared to cross.

Participating in E-Jihadism is seen as an important role by the Jihadi community, as is indicated by an official guide that has been shared on social media. It states that "It is upon any individual to consider himself as a media-mujahid, dedicating himself, his wealt[h] and his time [to] God."[12]. The embrace of E-Jihad is a successful attempt to both spread the Jihadist ideology as well as to weaponize sympathisers without making them cross physical and moral boundaries they might not be prepared to cross. This is done in relative secrecy as Jihadis have adopted a number of tools and methods to protect their (digital) identity. Ironically, most of them rely on Western encryption and anonymity techniques. Such tools are discussed on forums[13] and social media[14], and are often accompanied by well-written Arabic documents explaining their implementation and use[15]. Messaging applications with strong encryption, such as WhatsApp, Kik and Telegram, are favoured by Jihadis. Credentials for such applications are often shared in users' biographies or posts, and it is via these applications that recruitment, travel, and attack planning takes place. FBI Director James Comey has described this process as 'going dark' as surveillance agencies have difficulties keeping their eyes on targets after this has happened and recognize this step as a crucial turning point in the radicalisation of individuals[16].

3. Social Media Intelligence

Digital research methods entail an approach to doing research with online objects such as Twitter and Telegram via online objects such as hyperlinks and hashtags[17]. Here the studied object and the phenomenon for which it is used, such as elections, are examined by repurposing the object itself. While the dissemination network of E-Jihadism has a 'real world' counterpart, it is largely aimed at and acted out online. Digital methods can be used to gather information that can be made into actionable intelligence regarding the 'real world' phenomenon. However, the use of anonymity and encryption software means there are few options to identify 'real world' actors. That said, since many supporters are only active online, digital methods can be used for mapping out the dissemination network of E-Jihadism as such. However, digital methods are inherently limited to the object's affordances. Data gathered from specific digital objects is not just there already; they are designed in such a way that only certain information is stored, and can thus be scraped via tools, while other information is not[18]. Regardless of these limitations, open sources of information, such as social media, can be used to create OSINT/SOCMINT.

Information on social media platforms can be made into intelligence by recognizing patterns and objects within the (meta)data. A tweet, for example, consists of up to 33 pieces of metadata, such as the time it was posted

11 | Op. cit. Bartlett and Fisher 2015.
12 | Qtd. in op. cit. Fisher 2015, p.7.
13 | Hegghammer T., Interpersonal Trust on Jihadi Internet Forums, Norwegian Defence Research Establishment, 2014, p.18.
14 | Bartlett J., and Krasodomski-Jones A., online anonymity islamic state and Surveillance, Demos, 2015.
15 | Brantly A., and al-'Ubaydi, M., Extremist Forums Provide Digital OpSec Training, "CTC Sentinel", 2015, p.11.
16 | Berger J.M., Tailored Online Interventions: The Islamic State's Recruitment Strategy, "CTC Sentinel", 2015, p.21-22.
17 | Rogers R., Digital Methods, 2013, p.19.
18 | Weltevrede E., Repurposing Digital Methods, University of Amsterdam, 2016, p.3-4.

and the location it was sent from. Collecting and analysing such metadata, especially in combination with other data or information, can create actionable intelligence. Location-based information, for example, can be retrieved by analysing the content of tweets, posting patterns, and time zone metadata[19]. Within networks, the spread of specific content or digital objects can be analysed by looking at the frequency of sharing, the means of spreading, and the users who are sharing content[20]. Besides providing insight into the workings of the network on social media and the operationalization of others platforms, this method can also be applied to determine targets for censorship or surveillance. Lastly, Social Network Analysis can be used to map out and analyse user clusters and influential actors in complex networks.

A research project on Jihadi use of Twitter tried to define the number of active ISIS accounts, which was estimated to be between 46,000 and 70,000[21]. However, fewer were actually active at any given moment[22]. One in five selected English as their primary language, while three-quarters chose Arabic. The average amount of followers was 1,004, compared to the Twitter average of 208. Less than three-quarters had fewer than 500 followers[23]; just under half had fewer than 200 followers, and a quarter had fewer than 100 followers. This emphasizes the relatively small and cellular nature of ISIS networks on Twitter. On average, ISIS accounts follow 418 accounts, compared to the Twitter average of 108[24]. While they seem to be well connected compared to the Twitter average, this comparison is not representative as the average encompasses all accounts, including those hardly ever used. ISIS sympathisers are passionate about a specific subject they actively engage in. Thus, a more meaningful average to compare with would be a similar community such as a fan or activist group.

Several categories of Jihadi Twitter accounts have been identified: node accounts, i.e. generators of primary content, amplifiers which retweet content, and shoutout accounts that promote newly created accounts of suspended users[25] Nodes are the leading voices in the community; they operate in smaller or bigger clusters of followers with which they share anything from memes and news articles to official ISIS tweets and material, depending on the type of node account. Amplifiers retweet content from popular users, such as node accounts. Sometimes these accounts are not operated by humans, but function on their own as automated bots. In fact, Jihadis have developed apps to send out thousands of tweets via such bot accounts. They contain different links to the same content, using the same hashtag[26]. Shoutout accounts are vital to the survival of ISIS on Twitter. They introduce new pro-ISIS accounts and new iterations of suspended users, enabling them to quickly regain their old follower base. Shoutout accounts tend to have the largest following, which is indicative of their importance to the network[27]. The Jihadi Twitter network can be described as a distributed one, in which amplifier accounts disseminate content – originating from a few node accounts – to various clusters[28]. Within these clusters, accounts retweet content and send tweets of their own to their followers. These tweets contain the same hashtag, but a different link to the same content, for instance on a different platform or from a different uploader as the owners of the accounts download the content and then upload it themselves. These tweets are, in turn, retweeted by their followers on a much larger scale than the node and amplifier accounts can ever achieve[29]. Amplifier accounts are much more connected to the rest of the network, even more so than the node accounts. Because of their importance as connectors within the network, amplifier accounts are more likely to be suspended than other accounts, such as nodes or those of sympathisers. However, when this happens,

19 | Bartlett J., and Reynolds L., the state of the art 2015 a literature review of social media intelligence capabilities for counter terrorism, Demos, 2015, p.38-39.
20 | Ibid p.53.
21 | Berger J.M., and Morgan J., The ISIS Twitter Census Defining and describing the population of ISIS supporters on Twitter, Brookings Institute, 2015, p.2.
22 | Ibid p.7.
23 | Ibid p.30.
24 | Ibid p.32.
25 | Vidino L., and Hughes S., ISIS in America: From Retweets to Raqqa, George Washington University, 2015, p.ix.
26 | Berger J.M., and Stein J., ISIS: The State of Terror, HarperCollins UK, 2015, p.25;151.
27 | Ibid p.24.
28 | Shaheen J., Networks of Terror: How Daesh Uses Adaptive Social Networks to Spread its Message, NATO StratCL COE, 2015, p.11.
29 | Op. cit. Berger and Stein 2015, p.155.

their role is often taken over by one of their followers who simply retweet node accounts and start acquiring more followers[30].

Hashtags are used by Jihadis to disseminate content through the various communities the network consists of. In fact, one in every 3.7 ISIS tweets contains a hashtag[31]. The most frequently used hashtags are variations of the Arabic name for the Islamic State, representing 2.8% of all tweets containing hashtags. Despite being a relatively small percentage, no other hashtags come close to that usage. Variations of the name make up just over a quarter of the top 100 hashtags. Another 9% is related to Twitter suspensions and the rest relates to a variety of topics. In fact, 60% of the top 100 hashtags are not directly related to ISIS. Tweets are often accompanied by relevant hashtags, such as the title of the content or the name of the publishing media outlet, and a link to content. That way, interested individuals can easily find content they are looking for. Hashtags allow distributors to circumvent account suspension by providing a fixed point in cyberspace for connecting with interested parties. However, the centrality of hashtags also results in some of them being used to spread (anti-ISIS) noise[32], as activists try to disrupt the dissemination system by hijacking hashtags and 'trolling' ISIS by flooding the network with anti-ISIS content. Despite this, the use of hashtags has proven to be an effective content dissemination method because Twitter does not censor them, unlike accounts, and hashtag flooding is not nearly as frequent and consistent enough to have a lasting effect. Thus, there is no need for large following or official branding, which tends to lead to suspension. In fact, the more the disseminating accounts blend in, the better[33].

A little under half of all Jihadi tweets contain URLs[34]. Each link is shared 6.4 times on average and the top 10 are shared between 117 and 245 times[35]. Others found that 40% contained a URL and that 689 links were shared more than 100 times, with the top one being frequented 846 times[36]. Yet another research project established that 30 to 50% contain links[37]. While there is no definitive number on the frequency of tweets containing URLs, as this depends on the dataset used to assess this, for Jihadis it is generally higher than the Twitter average of 35%[38] and indicative of the importance of tweets as vehicles for disseminating (links to) content.

The only way to compile a full dataset of all links to content and disseminating accounts is to systematically monitor each hashtag[39]. Hashtags are a central element in a distributed network, on Twitter and other platforms. While accounts in the network are subject to suspension, and are thus fleeting objects, hashtags stay the same. Therefore, I will present findings based on 17 hashtags which, amongst other things, will show other hashtags used in combination with the 17 seed hashtags, and accounts using them. While this is by no means a full account of all hashtags used, it acts as a springboard in order to further similar projects.

Surprisingly little research has been done on the Jihadi use of Telegram, even though it has become the initial hub for disseminating propaganda[40]. Despite crackdowns on Jihadi channels after the Paris attacks, Jihadis now strongly favour Telegram, not least because censorship has been rare since[41]. At the time Telegram began blocking ISIS accounts, the official Arabic channel had over 16,000 followers and the two primary unofficial English accounts had a total of over 5,000[42]. Other high-profile

30 | Ibid p.13.
31 | Op. cit. Berger and Morgan 2015, p.20.
32 | Ibid p.56.
33 | Winter C., Documenting the Virtual 'Caliphate', Quilliam Foundation, 2015, p.11.
34 | Fisher A., and Prucha N., The Call-Up: The Roots of a Resilient and Persistent Jihadist Presence on Twitter, "Global ECCO", 2014, p.19.
35 | Ibid p.21.
36 | Op. cit. Berger and Morgan 2015, p.21.
37 | Op. cit. Shaheen 2015, p.10.
38 | Bartlett J., and Reynolds L.,The state of the art 2015 a literature review of social media intelligence capabilities for counter terrorism, Demos, 2015, p.43.
39 | Op. cit. Winter 2015, p.12.
40 | Berger J.M., and Perez H., The Islamic State's Diminishing Returns on Twitter: How suspensions are limiting social networks of English-speaking ISIS supporters, George Washington University, 2016, p.18.
41 | Stalinsky S., and Sosnow R., Encryption Technology Embraced By ISIS, Al-Qaeda, Other Jihadis Reaches New Level With Increased Dependence on Apps, Software - Kik, Surespot, Telegram, Wickr, Detekt, TOR: Part IV - February-June 2015, MEMRI, 2015.
42 | Op. cit. Berger and Perez 2016, p.19.

channels are ISIS' Amaq Agency channel with over 9,000 subscribers; Fursan Al-Raf' (Knights of Upload), a channel with over 3,000 subscribers dedicated to uploading ISIS releases; and Global Islamic Media Front which counts over 1,000 members[43]. In these channels links to other Telegram groups and channels are shared that are not shared elsewhere. The difficulty of automated means of analysing Telegram, its inbuilt encryption techniques and its anonymity-centric architecture as well as the resulting lack of literature on the Jihadi use of the platform means a contribution needs to be made in this area. For this purpose, this paper presents findings based on eight Jihadist channels and one group, showing, among other things, the use of hashtags and links to Twitter, Telegram and other platforms.

> Several countermeasures have been taken to fight E-Jihadism. While some of these measures have proven effective on some platforms, no ultimate solution is yet in sight.

The use of social media plafroms for Jihadist purposes has led to fierce criticism. Especially the well-known ones such as YouTube, Facebook, and Twitter took the brunt of the criticism, but only the former two tried to actively ban Jihadis from the start[44]. Twitter, instead, claimed that "One man's terrorist is another man's freedom fighter"[45] and argued that the Jihadist using social media falls under the freedom of speech. While debates over censorship often involve the 'right to free speech' argument, it is important to note that it is fully within the right of social media companies to regulate speech on their own platform in any way they see fit, without any oversight or disclosure[46]. During the censorship debate that followed, those arguing for suspension claimed that the intelligence value of social media accounts was slim, since the content was highly regulated and often false propaganda. Opponents argued that it could be used to determine the identity and the number of Jihadi sympathisers. It was also argued that only a minor snippet of information was needed for it to have actionable intelligence value[47].

Twitter has occasionally suspended Jihadi accounts, and only after bad publicity made it a temporary issue for them did they increase the pressure for a while. However, after a video of the James Foley beheading surfaced on the platform in the summer of 2014, they adopted a more aggressive approach[48]. Later, Twitter announced that they removed 125,000 accounts in the latter half of 2015[49]. While targeting official accounts with large followings has had lasting success, Jihadis now use smaller accounts that fly under the radar or just use new iterations of suspended accounts[50]. However, suspension on Twitter does make the reach of ISIS accounts decline. It makes Jihadis spend more time rebuilding the network rather than using the network to spread content[51]. Suspensions have a concrete effect in limiting the reach and scope of Jihadi activity on social media, although they do not eliminate it totally. Critics who argue suspension is ineffective because content is still available fail to consider the qualitative side of suspension, in addition to the quantitative one, as the performance of the network is affected.

For Jihadis, suspension is not only seen as part of the deal, but also as a marker of identity, dedication, and respect. The amount of times one is suspended is indicated in the username, and the higher the number, the more respected the user is, as this shows his dedication to the cause. The first tweet of a new iteration of a suspended user is often an image of Twitter's suspension message, proving they are the owner of the old account. This is accompanied by a shoutout request, which

43 | Khayat M., Who Is Posting Islamic State (ISIS) Materials On The San Francisco-Based Internet Archive (Archive.org) - And What Can Be Done About It?, MEMRI Jihad and Terrorism Threat Monitor, 2015.
44 | Op. cit. Berger and Stein 2015, p.134.
45 | Qtd. in Ibid p.138.
46 | Op. cit. Berger and Morgan 2015, p.3.
47 | Op. cit. Berger and Stein 2015, p.144.
48 | Op. cit. Berger and Morgan 2015, p.23.
49 | Op. cit. Stalinsky and Sosnow 2015.
50 | Op. cit. Berger and Morgan 2015, p.23.
51 | Berger J.M., Resistible Force Meets Movable Object, Intelwire, 2014.

enables followers to come back[52]. In fact, one in five tweets is related to suspension and shoutout requests, and users who have been suspended tend to be far more active and popular than average Jihadi users[53]. Suspensions are a vital part of E-Jihadi identity[54] and taken as a form of empowerment and confirmation of a shared identity rather than a hindrance.

A definitive solution to E-Jihadism is probably a utopian idea, and while increased censorship will lead to increased resistance and E-Jihadism 'going dark', it will also make it harder for Jihadis to radicalize and recruit new people. Yet, some methods have been suggested to make a bigger and more lasting impact. The AIVD[55], for example, claims that a successful measure should tackle multiple features of the network simultaneously. Taking down individual websites, forums, and social media accounts hardly has a lasting effect as this is anticipated by the Jihadis[56]. The more that is removed or made inaccessible at the same time, the better; otherwise there are still plenty of avenues for reconnecting the ties. Communities of interconnected users and bridges between them and other communities can be targeted for suspension as well as inactive or 'sleeping' accounts in the network[57]. However, while a simultaneous disruption of the entire network could prove to be a fatal blow, it is unlikely that a new network would not be formed one way or another especially since connections have likely been made in secret on platforms which are hard to monitor. Still, Facebook and many others have had lasting success in removing Jihadis from their services, and so could have Twitter and Telegram as they have been successful in temporarily removing Jihadis already. However, such a disruption could result in the establishment of new online networks that are even harder to monitor. This is not to say that no censorship should ever happen – surely, there is a need to protect society from Jihadi influence. But, when enforcing such a policy, its consequences, unclear as they may be, should be critically considered, too. That said, whether a policy of censorship, intelligence gathering, or something in between is adopted, there is a need to map E-Jihadism in all its aspects.

52 | Op. cit. Vidino and Hughes 2015, p.24.

53 | Op. cit. Berger and Morgan 2015, p.34.

54 | Pearson E., Wiliyat Twitter And The Battle Against Islamic State's Twitter Jihad, Vox Pol, 2015.

55 | Dutch General Intelligence and Security Service.

56 | AIVD, Jihadism On The Web A Breeding Ground For Jihad In The Modern Age, 2014, p.15.

57 | Op. cit. Shaheen 2015, p.23.

5. Twitter Hashtags and Telegram Channels

Table 1 shows 17 hashtags listed on Halummu, an ISIS blog. They are the seed hashtags used to gather tweets. While these hashtags only provide insight into a part of the network – since there are other seed hashtags that could be selected – the fact that they are listed on the homepage of an ISIS site indicates their importance to Jihadis and their value as research objects. Moreover, defining another set of seed hashtags would require arbitrary criteria to be applied during the selection process.

Seven hashtags are in English and ten are in Arabic. For the Arabic hashtags, the English translation[58] is provided in brackets. These hashtags mostly refer to various production offices and general ISIS news. One hashtag is dedicated to spreading invitation links to Telegram channels.

These 17 seed hashtags were scraped from 3 May, 2016 onwards using the Digital Methods Initiative's Twitter Capture and Analysis Tool (TCAT). They were subsequently extracted from TCAT and analysed for a period of one week, ranging from Sunday, 8 May to Saturday, 14 May, 2016. While a longer monitoring period could potentially produce more representative findings, a week-long snapshot was chosen due to time constraints.

Table 2 shows four English and four Arabic Telegram channels, as well as the Arabic group that were included in the analysis. The channels were chosen based on non-statistically relevant random sampling from a number of other available channels. Three of the four English channels were chosen because of their orientation towards digital media; the remaining one was selected as it is the only English channel which seems to be operated by an individual. The four Arabic channels were chosen because they post Jihadi news, content, and links to

58 | Via Google Translate.

content. Unfortunately, without proper understanding of Arabic and Jihadi politics, it is hard to identify who exactly operates the channel and what specific purpose the channel serves. The ISSDARAT group, who's name refers to an ISIS website, was chosen as this is the only group available and thus provides an interesting addition as a research object.

Table 1. Seventeen seed hashtags

#AjnadMediaProduction	#قناة_نشر [#Channel_publisher]
#AlBayanRadio	#مؤسسة_الفرقان [#Furqan_Foundation]
#AlFurqanMedia	#مركز_الحياة_للإعلام [#Life_Center_for_Media]
#AlHayatMediaCenter	#أخبار_الخلافة [#News_succession]
#AmaqAgency	#إذاعة_البيان [#Radio_statement]
#Dabiq	#النشرة_الإخبارية [#The_news]
#IslamicState	#الدولة_الإسلامية [#Islamic_country]
	#تقارير_الولايات [#Reports_US]
	#دولة_الخلافة [#Caliphate_state]
	#الدولة_الخلافة_الإسلامية [#The_Islamic_caliphate]

Table 2. Telegram channels and groups

GIMF الجبهة الإعلامية [GIMF Media Front]
Link Up
Mustafa Al Iraqi
United Cyber Caliphate
قناة بيارق الدولة [Channel banners of State]
نشر	#مؤسسة الوفاء [Publisher	#Foundation fulfilled]
وكالة أعماق [Agency depths]
مؤسسة الثبات/عام [Stability Foundation / General]
ISSDARAT

The channels and the group were scraped manually[59]. Similarly to Twitter, the same week-long period was chosen on the assumption that this might yield similar findings which could be compared and analysed.

The findings show tweets containing the seed hashtags are often accompanied by links. For some hashtags upwards of 40% do so. For most, this is around 70%, and for some hashtags almost all tweets contain links. This is much more than the less than half which other researchers found[60], most likely due to the difference between their datasets – which contained all tweets posted by Jihadi accounts – and mine, which only included tweets containing a hashtag. This is a strong indicator of the importance of hashtags in the dissemination system. Even when tweets do not contain links, hashtags are used as a vehicle for disseminating news or commentaries. Both tweets containing links and tweets without links are often retweeted. Usually around 30% of all tweets are retweets, and for some hashtags this goes up to 60%. While discussing tweets containing URLs in general (my dataset also encompassed tweets without URLs), Bartlett and Reynolds found 25 to 40% of those tweets were retweeted[61]. However, in the case of E-Jihadism, this is slightly higher, even with the URL-less tweets included. For some seed hashtags, the top retweets are reposted fewer than a dozen times and for others hundreds of times, making up a significant portion of all tweets in some cases. These numbers are similar to those described by Berger and Morgan[62].

Findings showed the top 10 retweets for each seed hashtag often have the same content, but stem from a different publisher, and link to the same content on different platforms. Some of the original publishers appear in the top 10 multiple times, indicating their importance in the network. These could be described as "Jihadi producers"[63], or node accounts. The findings show some of the top retweets link to Telegram channels, and one seed hashtag (#قناة_نشر [#Channel_publisher]) is even dedicated to this purpose. Shoutout requests are also common in top retweets. Together, this clearly shows a part of the interconnectedness of platforms and accounts

59 | The methodology as well as the resulting 'raw' data is available on request.

60 | Op. cit. Berger and Morgan 2015, p.21.; Op. cit. Fisher and Prucha 2014, p.19.; Op. cit. Shahee, 2015, p.10.

61 | Op. cit. Bartlett and Reynolds 2015, p.43.

62 | Op. cit. Berger and Morgan 2015, p.21.

63 | Op. cit. AIVD 2014, p.18.

that makes up the swarmcast which is so vital to the survival of E-Jihadism.

Hundreds, and in some cases over a thousand hashtags are used in combination with the individual seed hashtags, but only a few seem to dominate the network as a whole. These top hashtags are often different names for ISIS or general hashtags used for spreading the content. Some of them are specific to Jihadism, while others are more general or totally unrelated. This piggy-backing on unrelated hashtags has been described before by Bartlett and Fisher. Anti-Jihadi hashtags are also commonly used with Jihadi hashtags in order to appear in the results of those looking for the Jihadi content, with the aim of deradicalization or trolling. In fact, some anti-Jihadi accounts use the Jihadi hashtags much more than Jihadi accounts solely for the purpose of flooding their dissemination network. This too has been observed before[64]. Berger and Morgan claimed the most used hashtags are variations of names for ISIS, and that no other hashtags come close to that usage[65]. However, while the former is confirmed in the findings, anti-Jihadi, Jihadi-specific, and unrelated hashtags are more common than different names for some of the seed hashtags. While Berger and Morgan were talking about the top 100 hashtags, they found 9% of those hashtags referred to shoutouts[66]; however, none were found in the top 20 hashtags used with the seed hashtags. Furthermore, they found 60% of the top 100 are not directly related to ISIS[67], but no such results were found in the top 20. They did find Jihadi hashtags contained a large amount of anti-Jihadi noise[68], which corresponds with my findings for some, but not all of the seed hashtags. While English seed hashtags showed some Arabic hashtags in the top 20, hardly any English hashtags showed up in the top 20 of Arabic seed hashtags. Despite the findings showing many users set their device language settings to English, even those using the Arabic hashtags, there seems to be Arabic hashtag dominance. Berger and Morgan, on the other hand, claimed a mixture was common[69], although they were talking about tweets and hashtags, not hashtags themselves.

Some accounts that use the seed hashtags most appear in the top 10 for several seed hashtags, suggesting their importance in the network. Again, they can be identified as node accounts or 'Jihadi producers'. Suspended users, in some cases, make up half of the top 10 accounts which use the seed hashtags most. They are most likely Jihadis whose frequent occurrence in the dataset suggests that the usage of hashtags is required since establishing high amounts of followers proves difficult; within a week after the analysed period, many of the accounts were already suspended. Those that were not, for the most part, did not acquire a significant amount of new followers and some did not even have a noteworthy amount of followers to begin with, but did tweet hashtags and links a lot. However, some significantly increased their amount of followers. Berger and Morgan found the average amount of followers of Jihadi accounts to be over 1,000[70], which is much higher than the average in my findings – which also include non-Jihadi accounts, some of which have much higher numbers of followers. But even the average amount of followers of the top 10 users who tweet the seed hashtag most do not come close to that number, excluding some anti-Jihadism accounts. This decrease is likely due to the effects of suspension, as described before by Berger and Perez[71]. Many of the suspended accounts did not have large amounts of followers and had seemingly random names. This suggests that these accounts might be used as discardable accounts for disseminating content through hashtags, for which no followers are needed. The low follower and high tweet counts are a further indication of the role of these accounts as channels for publishing content via hashtags. Different iterations of the same Twitter account did seem to have closely matching and relatively high follower numbers, exactly as Vidino and Hughes described[72]. This proves that shoutout accounts are still essential in maintaining the network. These accounts are also more likely

64 | Berger J.M., Reflections Of A Troll, Intelwire, 2013.
65 | Op. cit. Berger and Morgan 2015, p.20.
66 | Ibid p.20.
67 | Ibid p.20.
68 | Ibid p.56.
69 | Ibid p.14.
70 | Ibid p.30.
71 | Op. cit. Berger and Perez 2016, p.7.
72 | Op. cit. Vidino and Hughes 2015, p.24.

to be retweeted or mentioned, as their function is more interactive than that of the discardable accounts. Despite their presence, they seem to be outnumbered by the discardable accounts, probably because hashtags provide an easier way to overcome the follower and suspension problem.

> “ The reliance on hashtags as a central point in a distributed network also results in them being used by anti-Jihadists who either troll them or aim at counter radicalization.

The reliance on hashtags as a central point in a distributed network also results in them being used by anti-Jihadists who either troll them or aim at counter radicalization. In some cases, only a few accounts, or a small group of accounts, tweet certain hashtags a lot in combination with the seed hashtag. This indicates a coordinated effort with a specific program. While this is more often the case for anti-Jihadism hashtags, pro-Jihadism programs have also been observed, for instance a French Jihadi hashtag cluster has been found. While clusters of accounts have been identified in Jihadi networks[73], no analysis of such anti-Jihadism networks has been done and neither has an analysis of Jihadi hashtag clusters. The anti-Jihadism accounts tend to have a large following and individual anti-Jihadism accounts tweet the seed hashtags much more than individual Jihadi accounts. The same holds for troll-accounts, although they tend to have few or no followers at all. This is due to the need for Jihadi accounts to post interesting and new content, while the other accounts can posts repetitive images and tweets since their aim is not to attract sympathisers but to de-radicalize and disrupt the network. Some of these accounts seem to be related, and like the Jihadi accounts, they have similar names and tweets. Again, such coordinated efforts by both pro and anti-Jihadist parties have not been analysed in the field.

73 | Op. cit. Berger and Stein 2015, p.14.

Between a dozen and a few hundred posts were shared via Telegram during the monitored week, depending on the channel. Many of those posts, upwards of 20%, but usually around 50 and sometimes up to 90%, were downloadable files. The amount of links in the posts varied greatly per channel. Sometimes only a small percentage of links to posts were found, but other times the amount of links doubled that of the posts. The safety Telegram offers means it is used as an initial dissemination hub for links, downloadable content, channels, and accounts on Telegram and Twitter. Many links to various formats of the same document on different platforms are shared, accompanied by requests to disseminate this content, specifically on Twitter. While content is also spread together with hashtags, they seem to have a less important status on Telegram than on Twitter. This is likely due to the lack of censorship on Telegram. Besides being used to share content, Telegram is also utilised to create connections in the Jihadi network. Users are actively encouraged to join platforms, follow accounts, and invite their friends. “Link Up”, the name of one of the channels, speaks volumes about Telegram’s purpose in this respect. Both active accounts and backup accounts are shared here, some of which are requested not to be shared on other platforms. Thus, the network stays clustered in platform-specific cells, which allows it to survive, even under the pressure of censorship. Forwarded posts are rarer than links and files; however, this varies per channel. For some channels, they make up less than 10% of all posts, while for others, they account for up to 90%. Only a few channels are forwarded to the seed channels, and some are forwarded to multiple channels. In some seed channels, only a few channels are forwarded many times more than others. Some of these forwarded channels have very similar names. This suggests a relative importance of a few (related) ones which could be identified as node accounts on Telegram, while the forwarding channels could be categorized as amplifier accounts.

Telegram is also a place for discussion, as groups provide a secure place of communication and, possibly, further radicalization. The group conversation was dominated by a few users and about 15% of all users were active in the chat during the monitored period. While the posts in the group reached a much higher volume, it had a similar

number of – and therefore relatively few – file and link shares, and forwarded posts. Hashtags were hardly ever used in the group.

The undirected approach, which is ascribed to the swarmcast, is not entirely true for Telegram. Since Telegram channels have a one-way, top-down architecture, where those in it are instructed to do or not to do certain things. Similarly, group conversations are dominated by a few and participated in by some members of the group only.

By using Digital Methods, E-Jihadism can be mapped by analysing the spread of specific content such as URLs via hashtags and Telegram channels. Such a method was applied and expanded on; however, the tools for gathering and analysing data are inherently limited, and so is the method.

One of the major limitations on Twitter is suspension, and users that do not or no longer exist, presumably due to the changing of usernames. This makes it impossible to analyse what kind of account one is looking at. Furthermore, Twitter automatically converts hyperlinks into t.co links, which means it is hard to get statistics on what platforms are linked to, as the only way to analyse them would be to manually open these links. More severe limitations were related to TCAT. This included the wrong query input for one of the seed hashtags. While such a mistake is easily spotted in a language one understands, it is much easier to miss such a mistake if one is analysing a language that uses a different alphabet. Another limitation is that TCAT does not allow tweets with the same content, but different links and/or uploaders, to be analysed easily. A tactic often used by Jihadis. Analysing this tactic would give enormous insight into the volume of disseminating accounts, as well as unique links used. While retweets show part of the picture, tweets which are not retweets, but have the same content and different links, present an unexplored area of study whose size is unknown.

The most limiting element in analysing Telegram is the application itself. The one-way communication architecture of Telegram channels, the inability to see who else is in the channel, and the lack of data extraction and analysis tools provide limited means for studying the platform. It is also impossible to copy the biography, the name of groups and the text in the profile picture other than by hand, using an Arabic keyboard. Furthermore, links to Telegram channels were often broken, presumably because the channel had been deleted or expired – since shared links can be set to function only for a limited amount of time. Sometimes a warning was given if this was the case. A number of joined channels were removed, or removed me, as access via the Desktop Client was impossible. Some of these channels are still accessible via the iOS client, but only the content that has already been downloaded to the device can be seen. This is a serious limitation for research purposes, as objects can suddenly become inaccessible altogether or only accessible through the mobile version, via which manual data extraction is a more elaborate and time consuming process than the desktop version.

The use of translating services such as Google Translate can provide enough information to get an idea of what the object you are looking at actually is. However, this method is not suitable for content analysis in many cases. While it is relatively simple to identify objects such as hashtags and links, even in Arabic texts, much of the nuance is lost after translating them. This makes even simple objects such as hashtags subject to limited possibilities for analysis and prone to misinterpretation. However, when combining translated texts with hashtags and hyperlinks, and analysing visual objects such as biographies, profile pictures and files, it is possible to make sense of Arabic objects.

Gathering literature on E-Jihadism and getting access to research objects proved difficult. Intelligence agencies are likely to have done much more in-house research on this subject and have access to research objects and methods of analysis; however, none of them are publicly available. Commercial institutions such as MEMRI and SITE publish articles on the subject, but most of them are protected by proprietary rights. Despite many emails, calls, and even an official request for specific articles, none were provided, despite the fact that their sites stated that articles are available to students on request. A request to

get access to Telegram channels did not prove successful either.

Conclusion

This article set out to use and reflect on digital research methods to map out the Islamic State's online dissemination network on Twitter and Telegram. Tweets containing one of seventeen ISIS-related hashtags and posts in eight Telegram channels and one group were gathered and analysed. A number of elements of the network could be mapped out using this method; however, some limitations became apparent.

The Twitter-related findings showed hashtags on Twitter are used by various categories of accounts as vehicles for the dissemination of links to content. They are, above all, a stepping stone to more in-depth research. Commonly used hashtags can be carefully selected for further monitoring. So can the accounts which use them, and accounts which are retweeted, or post content a lot. The connection between these accounts can be mapped and analysed by looking at follower relations. Links can be analysed more systematically to gather objects for further research. Specifically linked to Telegram channels on Twitter, other Jihadi accounts, and links to other platforms and accounts which upload to them can be investigated. Lastly, content analysis of tweets using a certain hashtag and corresponding Telegram channels might produce interesting findings.

The Telegram-related findings showed it is used as an initial point for disseminating content and connecting with networks in the swarmcast. Telegram channels and groups forwarded within Telegram, and those linked to on Twitter are interesting objects for further research. Content analysis of posts and downloadable files along with a more in-depth look at the dissemination of links, within such channels and groups are important avenues for further research as well. A comparison with related hashtags on Twitter could yield interesting findings as to which accounts tweet content after it has been released on Telegram. Hashtags used here can also be investigated further; while they seem of relatively little value on Telegram, they might be more intensively used on Twitter. Lastly, groups offer insight into the actor dynamics of in E-Jihadism.

Digital methods provide a means to map out the Islamic State's online dissemination network to some extent. The network could be further examined if the recommendations for future research are incorporated and the analysis would also include the third most popular platform - forums. However, the use of encryption and anonymity techniques, the limited affordances of platforms, and the tools used for analysis present difficulties for getting actionable intelligence that could help put people behind bars as precise locations, IP addresses and identities are hard to determine via these methods. That said, this paper did not intend to make such an attempt, but rather reflect on the methods of mapping out E-Jihadism on Twitter and Telegram as such. ■

INTERVIEW WITH ONDREJ KREHEL

ONDREJ KREHEL
is the CEO and Founder of LIFARS LLC, an international cybersecurity and digital forensics firm. He's the former Chief Information Security Officer of Identity Theft 911, US premier identity theft recovery and data breach management service. He previously conducted forensics investigations and managed the cyber security department at Stroz Friedberg and the Loews Corporation. With two decades of experience in computer security and digital forensics, he has launched investigations into a broad range of IT security matters—from hacker attacks to data breaches to intellectual property theft. He holds an M.S. degree in Mathematical Physics from Comenius University in Bratislava and an Engineering Diploma from Technical University in Zvolen, Slovakia. Krehel is a frequent speaker at industry events and author on matters related to information security and computer forensics.

Could you briefly tell us about the required cyber-security policies and procedures in the U.S and in Central Eastern Europe(CEE)?

The ability to legally defend and investigate cybercrime is perhaps the biggest difference between the U.S and the CEE have different approach towards data protection and information security laws.

The U.S cybersecurity is driven by legal requirements, such as data breach notification laws and by regulatory frameworks that are based on each industry's standard. On a federal law, the U.S preserves a sectoral industry approach towards cybersecurity and data protection laws where some industries are covered and others are not. For example, The Health Insurance Portability and Accountability Act (HIPAA) is a federal law, specifically for healthcare information. It protects the confidentiality of healthcare information and help healthcare industry.

However, the CEE follows legal and regulatory requirements that are not industry specific but are more globally standardized. The CEE's cybersecurity policies are usually from the EU and the EU has more all-encompassing privacy law. The EU has EU Data Protection Directive which is designed to protect individual privacy and personal data. Data protection in the EU is considered to be a human right and that is why it is more regulated by wide-ranging, comprehensive legislation.

How do companies in the CEE and those in the U.S invest differently in cybersecurity issues?

Recently, the U.S market has been focusing on detecting cybercrimes and responding to them, while the CEE market is focusing prevention and event correlation. Most of the organizations in the CEE are not ready for massive attacks outside of technical measures. However, as security threats continued to grow, I believe the CEE region saw a greater need in detection and response. A cohesive approach of prevention, detection, and response is getting much attention for companies in the CEE. Currently, companies in U.S is at budget hunting for incident response and are investing more on cybersecurity and privacy insurance policies.

What are the emerging cyber threats?

I would have to say ransomware and cyber extortion. Ransomware is gaining a great momentum due to the fact that attackers can secure fast payment of the ransom.

While it is not a totally new threat, ransomware has become one of the popular cyber threats nowadays as you can easily find cyber extortion and ransomware cases making the news. It is profitable for attackers at the moment and it doesn't seem like it will go away. Companies should be aware and employ resources to prepare for an attack.

Why was QuBit created and what is the aim of this community?

QuBit Conference was created in order to build a cybersecurity community event for the industry professionals, government and academics. Its mission is to be a respected industry conference ensuring its audience about valuable and educative content, open debates, friendly atmosphere and community spirit, rather than to be a place where businesses try to promote their services. The conference brings cyber security experts, managers, and decision makers together to create a Central European hub for sharing new ideas, best practices, and real life stories for advancing the security conversation forward through education, discussion, and relationship building.

As cybercrime continues to grow, QuBit tries to offer real solutions and share concrete ideas on how to deal with constantly growing cyber threats. Emerging threats in cybersecurity industry are presented through case studies and educational sessions and this raises the awareness in the field of cyber security.

QuBit offers different types of training. How do you find this training to be crucial in our current environment?

Training of cybersecurity professionals is very important; no army can claim victory without a training. QuBit offers several highly technical courses and trainings in order to provide affordable hands-on education and practices led by community experts from national CSIRT, military and other well technically equipped organizations.

QuBit also supports local universities in cybersecurity education. Currently, there are only few limited academic education programs for young security aspirants. By organizing student contests, public security awareness projects, and other activities, Qubit helps young students to be prepared in the early stage.

Why does LIFARS participate in the QuBit conference?

LIFARS has been assisting QuBit conference since the beginning. Founders of LIFARS are from the CEE region and we always try to contribute to the community. Moreover, LIFARS heavily promotes international collaboration to fight cybercrime and Prague is a great location to do so as it is located in Central Europe. LIFARS doesn't consider QuBit to be a place to promote our services. We believe it is a place where industry professionals share their knowledge to support the growth of new ideas in cybersecurity industry.

What is the future of cybersecurity in the CEE?

Legal frameworks for cybersecurity are getting much attention and eventually the cyber legal system will be established in the CEE region. Currently, enterprises in the CEE are challenged to hunt bad employees who try to steal data from them, as the legal system for cybersecurity has not been completely established. Like in the U.S, data protection should be more governed by market forces to solve these issues. There have actually been signs that show progresses on cybersecurity policies, such as the Directive on Security of Network and Information Systems (NIS Directive) that was adopted by the EU early this summer. I believe this was the first step to respond to cyber threats and cybersecurity incidents they have been facing. In the future, cybersecurity industry in the CEE should focus more on finding proper ways for businesses and corporations to protect their data and to avoid security risks. ■

OPINION

CYBER CHALLENGES: FUTURE DIRECTION FOR INNOVATIVE INSURANCE COMPANIES

DARIUSZ GOŁĘBIEWSKI
is associated with the PZU Group since 2004. He was responsible for risk engineering from 2009 to 2015. Since 2015 he has been running the project entitled "PZU LAB Research and Development Center" as Team Manager. Graduate of the Electrical Engineering and Automation Faculty at the Technical University of Gdańsk, Ph.D. in engineering sciences with a specialization in modeling the risk posed by power sector facilities for insurance purposes. Graduate of the Master of Business Administration program in the Business School at the Technical University of Warsaw. Designer of a proprietary methodology to analyze insurance risk known as Insurance Risk Analysis Methodology (IRAM). Author of many publications on insuring elevated risk facilities, critical infrastructure and risk management.

IZABELA LEWANDOWSKA-WIŚNIEWSKA
is currently participating in the Cybersecurity Project in the PZU Lab as coordinator. She is an implementation Specialist, Agent, Trainer and Auditor of management systems regarding safety, environmental issues, quality, CSR, PSM, IWAY, EMAS, OHSAS, AQAP and risk management. As project management specialist in PSM technical safety, she deals with systemic solutions for corporate clients and innovation projects, on Critical Infrastructure, Elevated and High Risk Business Units, risk management analyses and business continuity. She is also a Safety and OSH manager with many years of experience in preventive measures and systemic solutions, safety-related innovations in multiple areas and sectors, including industry, logistics and the military. Graduate of the Chemical and Process Engineering Faculty, post-graduate courses specializing in process-related safety.

Cybersecurity is presently one of the high-priority challenges of our times. The ubiquitous Internet of Things, the generation brought up in the era of digitization, and process automation are signs of the times. All these elements inevitably lead to cyber factors affecting all branches of industry, thereby contributing to developments in control systems. However, this progress entails a risk that it may materialize in the form of cyberattacks that will threaten and potentially interfere in industrial processes. Industry continually fails to grasp the gravity of this problem. The impact of a cyberattack on industrial facilities may be catastrophic not only to property, employee lives and their wellbeing or the environment, but more importantly to critical infrastructure whose disruptions may destabilize the continuity of operation of nations' crucial systems such as electric power transmission. Cyberattacks may cause industrial disasters and ultimately move acts of war to cyberspace. Over the last decade we have observed a spike in cyberattacks against companies in all industrial sectors both in Poland and across the globe. Industrial automation and control has become a focal point for cybercrime and cyber terrorism because they can inflict large-scale financial losses and disrupt processes in manufacturing companies.

Presently, a hacker can mount a cyberattack from any given venue on the globe – that is why cybercriminals often have a pervading sense of impunity. Politically or ideologically motivated (terrorism) cyberattacks against industrial facilities indicate that the threat to critical infrastructure is very real. Preparing and carrying out an attack does not have such a high price tag as the cost of employing conventional methods like sabotage for instance. The intended propaganda effect may be pronounced, while the political and criminal implications for the perpetrators are largely inconsequential since tracing the origins of the attack is extremely difficult. The very large number of industrial plants, critical infrastructure facilities and their economic significance make them particularly susceptible to terrorist attacks, including cyberattacks.

We Conduct Analyses and Devise Solutions

The issue of cyber threats is particularly important to insurance companies due to the emergence of new technologies and threats as well as the necessity of offering customized insurance policies, such as Cyber Policies, to their clients. As Poland's leading insurance company, we are working on rolling out dedicated and highly innovative insurance solutions to protect firms

against the consequences of cyberattacks on their critical infrastructures, including industrial installations. PZU LAB has been set up specifically for the purpose of taking such actions. Insurance companies have observed more pronounced interest in taking out insurance cover to offset possible negative impacts associated with the loss and recovery of proprietary and client sensitive data. However, the interest taken in this type of cover among prospective clients does suggest that insurance companies must do a lot more to hone their offering. The development of new technologies and the Web leads to the emergence of a host of new cyber risks, irrespective of industry and company size. These risks were unknown a short time ago. The magnitude of the repercussions inflicted by a cyberattack may vary from the loss or sale of information, the loss of reputation to terrorist attacks, property damage (fire, explosion, etc.) and human fatalities. That is why it is advisable to approach the subject of cyber risks comprehensively and consider transferring the risks posed by the following threats to an insurance company:

- Cyber terrorism in industry;
- Hostile takeover of decision-making centres, e.g. a system that controls an industrial process;
- Loss and destruction of technical data, e.g. control system databases.
- Data leak (commercial and personal data with confidentiality clauses);
- Loss of profit as a consequence of an information system attack;
- Incurring incremental costs associated with responding to computer attacks;
- Loss of positive corporate image;
- Costs of business recovery following a cyberattack.

The decision concerning the scope of insurance cover should be preceded with a meticulous risk analysis that identifies the threats related to cyber risks. Entities that specialize in this subject matter have begun to appear in Poland. Insurance companies also appreciate the gravity of this problem and are setting up specialized units to support their clients in a cyber risk analysis. The added value offered by insurers will probably increase on a much larger scale in the coming years. Third party experts and insurance specialists will offer professional support and furnish expertise concerning a given company's vulnerability to cyber threats; they will conduct analyses and propose safeguards and solutions, risk monitoring tools, and the appropriate protection bundle; and if a loss occurs, they will provide assistance during the claims handling stage.

Cyber Threats and Control Systems: Cyber Industry

Unfortunately, so far insurance companies have given little consideration to the security of systems controlling industrial installations where the consequences of unauthorized access (an attack) may be considerably graver compared to a loss of data. Jointly with its reputable partners in Poland, PZU LAB has commenced a research and development project on cybersecurity. The R&D work has started by devising a methodology for analysing the risks posed by cyber threats to industrial clients. This methodology will contribute to the creation of a tool to support Polish businesses in managing cyber risk, thus enhancing their level of operational security. "PZU Cyber Industry" consists of the following elements:

- A computer system based on the methodology for ICT critical structure protection that allows the vulnerability of corporate architecture and ERP systems to be examined.
- A tool to monitor the metering and control system in industrial installations in real time as well as to detect breaches that may disrupt an industrial process and, in consequence, cause damage and operational downtime.
- A methodology for analysing the vulnerability of industrial infrastructure to cyberattacks.
- A computer system to test for the vulnerability of the control system structure.

PZU LAB's engineers will deploy the above instruments in order to provide input to make an informed insurance decision, give information on vulnerabilities and methods of mitigating risk, and ensure constant oversight of industrial installations.

Cyber Insurance Offerings Must Be Comprehensive

There are modular cyber insurance bundles on the global insurance market offering extensive insurance cover to protect a business against claims for damages, losses, information leaks and disclosures. These insurance bundles offer safeguards to cover the costs of hiring technical experts, data recovery, and public image restoration. However, we can do more than that. Presently, the market provides only inflexible and conventional solutions. Ensuring information and communication security calls for a set of organizational and technical measures to minimize the risk of disrupting operations and unauthorized actions adversely affecting systems, ICT networks as well as measurement and control instruments. The current state of cybersecurity of industrial systems and the rapid technological development appear to favour cybercriminals and state-sponsored entities that specialise in launching attacks against the infrastructures of another country. Exceptional caution is required when handling and safeguarding critical data, especially in a time of terrorism that carries with it enormous potential losses, including the trust of business partners, and the possibility of squandering a company's reputation. The risk analysis conducted by an insurer's experts should therefore examine all three areas of cybersecurity activity of an insured business:

1. Organizational activity mainly encompasses the analysis of corporate architecture, primarily seeking to answer the question: who, why, to what extent, and where has access to a given device or a piece of information.

2. Operating activity involves the review of the ICS diagram, "tangential" points with the IT layer, and testing for systemic vulnerabilities to cyberattacks.

3. Technical activity takes into account the means and methods of active and organized cyberdefence.

Supporting Innovative Projects Is One of The Most Important Elements of Development: Witelo

Through Venture Capital (VC) funds, Witelo strives to pursue innovative projects from their early stage of development until they reach full operational capability allowing the business to expand. On the one hand, this entails the establishment of centres for development of innovative technologies in Poland that will help start-ups go global. On the other hand, this requires investments in the best VC funds that will support these hubs through their efforts. PZU supports the CYBERSEC Conference and the Kosciuszko Institute in their endeavour to turn Krakow into a centre for innovative cybersecurity solutions. That is why the Witelo project has become a partner of CYBERSEC Start-Up Days.

Sophisticated on-line diagnostics of damage / cyber threats to ICS systems and the associated methodology will become one of the key elements of "Industry 4.0" solutions as they attenuate the risk in ICS systems posed by cyber threats. The diagnostic system is the final layer facilitating the detection of cyberattacks if they happen to penetrate all the other layers of protection.

The cyber insurance market offering policies to cover the repercussions and ensuing negative impacts of a cyberattack may produce a desired outcome in the form of enhanced resistance of industrial installations to cyberattacks and a heightened level of cybersecurity. The transfer of cyber risk to insurance companies will allow businesses to offset the losses caused by a successful cyberattack. ■

thalesgroup.com/cic

Critical Information Systems and Cybersecurity

Wherever safety and security matter, we deliver

Mastering Critical Information and cybersecurity is the challenge of the 21st Century. Our mission is to help customers stay competitive and go beyond security to ensure resilient and high-performance critical information systems that integrate breakthrough technologies. Building on more than 40 years of experience, our team of 5,000 critical IT engineers, including 1,500 cybersecurity experts, offers you an end-to-end portfolio of solutions adapted to your specific needs across all sectors. We are a trusted partner of governmental bodies, critical infrastructure operators and companies. Every moment of every day, wherever safety and security are critical, Thales delivers.

Search: Thalesgroup

THALES

Together • Safer • Everywhere

SPECIAL REPORT

ADAPTIVE DEFENSE
A CAPABILITY MATURITY MODEL FRAMEWORK

ADAM PALMER
Adam Palmer, CISSP, JD, MBA, is a global cybersecurity policy and strategy leader. Adam is a former US Navy Officer, Prosecutor, and Manager of the U.N. Global Programme Against Cybercrime.

DR. PHILIPP AMANN
Dr. Philipp Amann, MSc, is the Senior Strategic Analyst, Head, Strategy Development Team at the EUROPOL, European Cybercrime Centre (EC3).

FOREWORD BY STEVEN WILSON, HEAD OF THE EUROPOL CYBERCRIME CENTRE (EC3)

From a law enforcement perspective, the current cybercrime landscape is characterized by increasingly aggressive and confrontational behaviour; attacks are becoming cross-platform compatible, more targeted, growing in scope, volume, number of victims and economic damage.

Cybercrime is now also being "industrialised" and is characterized by a division of labour with specialisation of specific services. This is driving a digital 'Cybercrime as-a-service' (CaaS) underground economy. This CaaS model represents a continuously evolving and modular industry that facilitates cybercrime and stimulates the innovation of tools and methods. By enabling a broad base of often unskilled, entry-level criminals and other actors to launch cyber attacks, the CaaS model gives disproportionate capabilities to attackers and creates an asymmetric risk for organizations in terms of risks, costs and criminal profits.

The growth of cybercrime and the increasing damage caused by attacks calls for innovative law enforcement approaches to prevention, protection and investigation. Such approaches not only need to be intelligence-led, agile and adaptive, but also require efficient public-private partnerships to respond to the dynamic, evolving and borderless nature of cybercrime in an equally diverse, coordinated and flexible manner.

An important aspect of public-private partnerships is the sharing of intelligence in a structured and standardised way among all relevant stakeholders with a view to building a comprehensive intelligence picture of cyber threats. This requires a common understanding of the type and category of intelligence that needs to be shared and its purpose. Equally important, it requires mutual trust as well as confidence by industry in law enforcement's ability to investigate both effectively and discretely.

For industry, besides establishing a base line cybersecurity and cyber resilience, a key strategic objective should be the adoption of a holistic and intelligence-led approach to protect and defend against cyber threats. This paper offers a systematic approach to achieving this by leveraging existing maturity model approaches to realise the ideal security posture of an Adaptive Defence. It describes a sustainable and resilient model that includes a circle of detection, prevention, analysis, and effective incident response to threats, underpinned by a continuous learning and improvement cycle.

Public-private partnerships and the systematic sharing of intelligence are some of the key aspects of an Adaptive Defence. The model specifically highlights the important role law enforcement plays in this context. It also supports novel and innovative, intelligence-led law enforcement responses to the growing threat of cybercrime and cyber threats in general.

I. OVERVIEW OF THE THREAT LANDSCAPE

While cyberattacks are becoming more advanced, the goal often remains the same – to steal information or money as quickly as possible. Attackers include state-sponsored threat actors or organized crime. While motivations may differ, the tools used are similar. Tactics, Techniques, and Procedures (TTP) may include social engineering, phishing, extortion, or malware attacks such as ransomware.

One recent report on a financial crime group provides a clear example of both advanced attacks and spearphishing. This crime group systematically targeted financial information in the biomedical and pharmaceutical sectors. The group used targeted and sophisticated emails to lure victims, who included CEOs, CFOs, research scientists, and lawyers, into providing their email credentials. The attackers then inserted themselves into the email trails, gaining access to privileged and market-sensitive information that would significantly impact the market value of the target companies. The attacks were successful without the use of any malware, relying on users to unwittingly use their email credentials on systems under the attacker's control. A lack of two-factor authentication on target victim systems made these attacks surprisingly simple yet highly effective.

Some attacks are now conducted without any malware. One example is when attackers leverage stolen credentials to access virtual private networks (VPN) infrastructure and connect to a network appearing to be a legitimate user. This can occur where attackers have successfully infiltrated the network in the past, and then compromised the domain credentials – in some cases, even compromising the two-factor authentication used for secure VPN connections. This allows attackers to return into the network using the corporate VPN, disguised as legitimate users thereby making detection difficult.

The recently discovered "CoreBot" malware is an example of the sophistication of social engineering attacks. CoreBot, a relatively new form of banking malware, uses a modular design that allows threat actors to customize the malware for different victim networks, as well as to install features, as needed, during an intrusion. CoreBot can perform browser injection, form-grabbing, and credential theft. It also includes a social engineering component to gather personal details from victims, information that is typically used as a secondary form of verification by financial institutions. This additional functionality may lead to higher success rates for financial fraud, identity theft, and even future social engineering attacks.

Attacks have also expanded to mobile devices. Researchers recently identified a series of Android trojan apps that are aimed at defrauding financial management institutions and service providers across the globe (North America, Europe, and Asia Pacific). Nicknamed "SlemBunk", these apps masquerade as common, popular applications and stay hidden after the initial running. They have the ability to phish for and harvest authentication credentials when banking and other similar apps are launched.

The continued sale and distribution of exploit kits and many spam campaigns demonstrates that attackers are still seeking easy compromises similar to "smash and grab" physical crimes in which the attackers do not intend to expand access beyond the infected system. While some exploit kit activities link to more advanced threat actors, the majority are associated with mass exploitation campaigns for monetary or personal information gain. Estimates of the cost of these threat activities are difficult to obtain and vary, but billions of U.S. dollars are likely lost globally. In some more egregious cases, there are lasting effects, where affected organizations realize the financial and reputational impact of compromises over the course of years. Though many of these attacks are opportunistic, some cybercrime actors may attempt to sell access to infected networks. Once access is sold, the activity may shift from opportunistic to a targeted attack.

Many cybercrime activities are facilitated by a professional underground "cybercrime as-a-service" industry that provides easy access to criminal products and services, and enables a broad base of often unskilled, entry-level criminals and other actors to launch cyberattacks. This gives disproportionate capabilities to attackers and creates an asymmetric risk for organizations in terms of risks, costs and criminal profits.

From a law enforcement perspective, the cybercrime landscape is characterized by increasingly aggressive and confrontational behavior. Specifically, law enforcement observes an increase in:

- ransomware and cryptoware
- use of remote access tools (RATs)
- card-not-present (CNP) fraud, which is likely to increase further since traditional cash-out destinations (like the U.S.A) for card-present (CP) fraud are starting to implement the EMV standard
- banking malware: targeting customers, but also banking infrastructure directly
- ATM malware: physical and logical attacks against ATM machines and ATM networks
- mobile malware
- social engineering

> "From a law enforcement perspective, the cybercrime landscape is characterized by increasingly aggressive and confrontational behavior.

Law enforcement has also observed the increasing criminal abuse of encryption and anonymity services and tools to mask identity and physical location, hide data, protect communication and obfuscate financial transactions. These developments call for an equally advanced, adaptive and holistic strategic approach as recommended by the Adaptive Defense model.

II. ADAPTIVE DEFENSE AND THE CAPABILITY MATURITY MODEL

A Capability Maturity Model (CMM) provides an organizational framework and methodology to build capacity and measure advancement in critical areas of cybersecurity. Maturity models are useful in guiding the development of processes and allocation of resources leading to an optimal state of readiness for a strategic objective. They can help assess current capability levels and identify areas of improvement using a risk-based assessment. Maturity models are also useful for evaluating compliance in the relevant legal and regulatory environment and for facilitating forward-looking analysis or "horizon scanning" for new emerging concerns and requirements.

Leveraging existing maturity model approaches[1] and related work[2], this paper offers additional, more granular, suggestions for achieving the ideal security posture of an "Adaptive Defense". The term "Adaptive Defense" summarizes a strategy that includes a holistic circle of detection, prevention, analysis, and effective incident response to threats, underpinned by a continuous learning and improvement cycle (capacity building). An Adaptive Defense describes a strong, sustainable and resilient model that also provides for a flexible approach to cybersecurity.

Benefits of using a CMM to develop an Adaptive Defense include:

- Establishing a holistic implementation framework with broad functionality
- Obtaining a snapshot of current readiness against various levels of maturity

1 | Cyber Security Capability Maturity Model v1.2, Global Cyber Security Capacity Centre, University of Oxford, December 2014, available at: https://www.sbs.ox.ac.uk/cybersecurity-capacity/system/files/CMM%20Version%201_2_0.pdf.

2 | Bodeau, D. J. and Graubart R., Cyber Resiliency Engineering Framework, MITRE Technical Report, September 2011, available at: https://www.mitre.org/sites/default/files/pdf/11_4436.pdf.

- Within a broader strategy, providing for a flexible approach that can be modified as technology or threats evolve
- Promoting a dynamic assessment and continuous improvement cycle

The most important concept of the CMM and Adaptive Defense is that each organization will have a specific goal level on the readiness spectrum. The goal will adapt according to changes in an organization's internal and external risk-based assessment. Part of the benefit of the CMM is the actual process to identify critical capability areas (domains) that correlate with a desired security readiness outcome. An organization should identify maturity levels within each domain. These are established by assessing the status quo and measuring progress along a continuum of risk-based preparedness from low readiness levels to full Adaptive Defense capability. The organization using a CMM should benchmark existing cybersecurity preparedness, evaluate core competencies, and create a framework that dynamically manages and measures improvement.

> "The term "Adaptive Defense" summarizes a strategy that includes a holistic circle of detection, prevention, analysis, and effective incident response to threats, underpinned by a continuous learning and improvement cycle.

Maturity level metrics provide a foundation for creating specific recommendations to increase capacity in areas of clearly identified need. Applied at the nation-state level, a CMM allows an aggregated view that can be gradually refined and expanded to all relevant national agencies, ministries, and stakeholders. Goals are likely to differ based on the characteristics of an organization such as size, structure, risk posture, and so on. There is not a "one size fits all" approach. The correct goal or appropriate maturity level for any domain must be based on the specific needs of each organization, consideration of the overall strategic objectives, and any relevant legislative and regulatory framework.

The heart of an adaptive defense is a dynamic and iterative process. It encourages holistic solutions and flexibility to achieve the appropriate levels of cyber resilience and readiness levels. The CMM approach supports organizations in building core capabilities by utilizing a defined methodology to steadily improve readiness levels. This is a bespoke approach. It focuses on specific risk areas and helps an organization ensure alignment across different domains. Narrowly tailored solutions can be applied to achieve specific measurable outcomes. By providing an accurate view of current readiness and a pathway toward improvement, the CMM process provides an operational framework for achieving an Adaptive Defense.

The core Adaptive Defense domains include Resilience, Detection, Coordination, Capacity, Cooperation. Each of these domains will be described in the following section and covered in more detail in section IV, which proposes a CMM-based approach to achieving an Adaptive Defense.

III. THE ESSENTIAL ELEMENTS OF AN "ADAPTIVE DEFENSE"

Resilience

Although cyberattacks are inevitable, an organization should have a defense that allows operations to continue with minimal disruption, and that provides adequate protection for critical assets. A data breach should not become a major "security incident". An organization must also learn from such events with a view to improving readiness levels. This is a form of resilience. Resilience is the ability of an organization to adapt to change and new risk environments, and to gain intelligence from past attacks. Resilience is not a single technical domain but a multi-faceted and multi-disciplinary domain. It includes the ability of an organization to not only prepare for and detect security threats, but to respond effectively in a timely manner, minimize damage, withstand disruptions, and to learn and adapt. If an organization takes weeks or months to mitigate a breach once it is detected, it has poor resilience.

Prevention is part of an Adaptive Defense. The resilience domain also includes prevention, but detection and effective incident response are the keys to resilience.

The resilience domain has a broader scope than basic "cyber hygiene" security. These are related, but separate, concepts. The U.S. Presidential Policy Directive 21 (PPD-21): Critical Infrastructure Security and Resilience defines "security" as reducing the risk by implementing defensive measures. "Resilience" is defined in the same directive as the ability to prepare for and adapt to (detect) changing conditions as well as the ability to withstand and recover rapidly from disruptions. Detection and incident response are the critical differentiators of resilience from mere defensive security. Frameworks that include resilience-based standards and recommendations include the ISO standards, the NIST U.S. security management framework and the Cyber Resiliency Engineering Framework[3].

Detection

Security includes not only identifying known threats, but the ability to detect and prevent unknown threats. An organization cannot prevent threats if it does not identify or detect a threat. The detection domain includes the response to threats once they are detected. Detection is the ability to make decisions based on a flexible programmatic approach that is based on actionable real-time information. This reduces mass amounts of information to focus areas based on direct understanding of threat actor methodologies and likely attack vectors.

Moreover, detection comprises the learning capabilities of an organization in terms of identifying and responding to threats. Managing intelligence and applying the knowledge gained from intelligence sources are critical in establishing adequate security and an Adaptive Defense. As such, detection is closely linked to resilience.

Coordination

Cybersecurity requires a multi-stakeholder and multi-faceted approach that is a harmonized response across multiple capability areas. The coordination domain includes organization of internal personnel, equipment, facilities, and plans necessary for collaboration and synchronization in planning for cybersecurity activities. This domain focuses on overall harmonization across an organization's security planning and response strategy both internally and externally. It also addresses questions of standardization, timeliness, and level of detail, and aims at enabling stakeholders at all levels.

Coordination is supported by clearly defined communication protocols; common taxonomies and standards for the description, exchange, and (automated) processing of information and intelligence. Coordination should include the creation of clearly defined points of contact for exchange of threat intelligence and management of risk mitigation activities – an example would be

3 | Op. cited Bodeau and Graubart.

the merger of the Security Operations Center (SOC) and the Computer Incident Response Team (CIRT).

Coordination is essential for effectively pooling the response capabilities of various stakeholders and avoiding conflict. A sound security plan should include mutually reinforcing activities that are synchronized across an organization. These activities should establish a front line of defense against immediate threats by enhancing shared situational awareness of network vulnerabilities, threats, and risks. By coordinating a security strategy across an organization, the organization increases its cyber resilience, strengthens its security environment, and reduces the risk of a threat causing significant harm.

Coordination is also a measure of organizational efficiency. Coordination can save costs by identifying operational areas that may be scalable and by avoiding unnecessary overlap and redundancies. During an evaluation of organizational needs, it may be possible to identify areas of commonality where the organization can implement shared controls or processes. This can avoid duplication and improve assurance that systems will be compatible. All of these activities improve the resilience and responsiveness or readiness of an organization.

Capacity

The capacity domain encompasses the ability of an organization to implement and execute its security strategy effectively. It is a measure of an organization's ability to promote the scale, quality, and implementation of cybersecurity initiatives across the organization. Using a risk-based approach, an organization may find that not every organizational entity needs to be at the same level of protection. Some entities may be categorized as "cyber key terrain" (CKT) assets. Capacity goals are adjusted within the maturity model based on an outcome of the risk-based assessment and identification of CKT.

A critical element of the capacity domain is the participation of senior decision makers across an organization to gain a clear understanding of CKT, security needs, and support for solutions. Capacity building should encompass not only vertical staff training but also horizontal efforts across an organization, focusing on the relevant aspects at each organizational level and in each functional area that are needed to support the security programme.

"Escalation" is a term now used in cybersecurity to describe the concept of an attacker entering a weak area of an organization's network and moving laterally into more secured areas. Because attackers have had devastating success using escalation to access and control networks, it has now become cliché to define an organization as only as strong as its weakest part. Coordination is critical to ensure that an acceptable cybersecurity baseline is established and that cybersecurity is harmonized at a necessary standard across an organization.

Cooperation

Public-private partnership (PPP), including cooperation with industry partners, the financial sector, academia, and law enforcement, plays an important role in increasing cybersecurity and resilience through raising awareness of threats, improving the overall intelligence picture, leveraging cybersecurity networks, and preparing adequate support for an effective response. Law enforcement, in particular, can be an effective partner that goes beyond detection. Successful cooperation and support for law enforcement operations can help tackle some criminal networks.

Cyberattacks will likely continue to grow in volume, scope, impact, and level of sophistication. The borderless nature of the attacks makes PPPs essential to address these unique challenges. A PPP model based on mutual trust, efficiency and effectiveness is needed whereby an organization will feel comfortable sharing information with government, and law enforcement investigates incidents discreetly and effectively. Accordingly, cooperation is a key to a successful Adaptive Defense.

IV. ACHIEVING AN ADAPTIVE DEFENSE

This section examines each core Adaptive Defense domain in detail. It is suggested to apply and evaluate each domain utilizing the CMM multi-stage evaluation process.

Applying The Capability Maturity Model

The initial analysis and planning for applying the CMM should include:

1. Conducting an assessment of each current operational area and its place on the CMM scale
2. Coordinating with internal stakeholders to apply a risk-based approach to establishing and evaluating the appropriate readiness level for each area
3. Identifying the steps necessary to move each area to the required level of security readiness
4. Identifying the ongoing requirements to maintain the appropriate readiness levels
5. Establishing an audit system with reporting requirements to verify maintenance of standards, identify deviations, and implement necessary adjustments on an ongoing basis
6. Implementing appropriate incentives and penalties
7. Providing appropriate protections of privacy and human rights
8. Establishing a long-term plan for building and maintaining capacity

Not every operational area within an organization needs the most advanced security. Identifying "security zones" or CKT is critical to identifying groups or assets that are worth defending or whose loss would be disruptive. Answering the questions "how good do you need to be", and "what type of cyber risk management program do you need" should be part of a collaborative discussion across all the relevant stakeholders in an organization. This should include the identification of all critical assets.

The modular step-by-step design of the CMM and not placing all groups in a single readiness track is intentional. There is a range of possible activities for each domain and these will vary across each organization – this is the foundation of a risk-based approach to creating an adaptive defense.

This approach is designed to enable a comprehensive, long-term, adaptive, and holistic approach to preventing and combating cyber threats and establishing a security readiness baseline. The focus is placed on understanding existing capabilities, ensuring that current initiatives are not duplicated, and implementing the necessary measures to assure long-term success.

A. Resilience

Resilience is the foundation of an effective cybersecurity programme – be it at national or organizational level. For the purpose of this paper and in support of the creation of an Adaptive Defense, resilience consists of four core areas:

1. Detection: Detection includes planning to evolve a security program beyond "basic cyber hygiene" to include intelligence from a range of sources and to make programmatic decisions based on actionable relevant information.

Threat intelligence should include awareness of known threat groups, their known attack methods, and anticipated attack vectors. Identifying the source of an attack can help you understand the objectives and motives of the attackers and why they are targeting your organization. From an Adaptive Defense standpoint, this means

that security programmes should evolve from passive monitoring to active "hunting" for evidence of threat actors within a network. This approach assumes the presence of an attacker that is using unknown intrusion techniques.

While intelligence can be considered one of the main elements, detection also encompasses other types of sources, producing different types of input, including data and information as well as intelligence, which typically involves human resources and interpretation. However, automation using artificial intelligence, machine learning, and Big Data analytics will play an increasingly important role in these areas and Adaptive Defense in general.

Essential elements of the detection domain are:

- Dynamic defenses to stop targeted, zero-day attacks, leveraging machine learning approaches
- Real-time protection to block data exfiltration attempts
- Integrated inbound and outbound filtering across protocols
- Accurate mechanisms that ensure a low false positive rate
- Global intelligence on advanced threats to protect local networks

To be effective, detection must be "intelligent" enough to identify and stop advanced polymorphic attacks hosted on dynamic, fast-changing domains. To address these advanced threats, real-time, dynamic and accurate analysis of network traffic and processes is critical. A fully mature Adaptive Defense aims to dynamically recognize new attacks in real time, without necessarily requiring prior knowledge of vulnerability, exploit or variant, and then prevent system compromise and data theft. This includes stopping data exfiltration and the ability to dynamically analyze network traffic to capture and detect zero-day malware. Equally important are real-time capabilities to stop the outbound communications of an attack and halt the flow of data to attackers. This needs to include advanced techniques to counter modern forms of steganography and other types of information hiding techniques in network traffic.

2. Prevention: Prevention includes activities to stop known and unknown threats from becoming security incidents. These activities include, among other things, protocols that are essential to a security programme and additional behavior-based heuristic detection capabilities that can prevent an attacker from exploiting an unknown vulnerability. Prevention includes a human dimension that focusses on minimizing threats and risks related to human behavior and exploits (such as social engineering) as well as learning and education.

Some of the main sub-domain controls for prevention and detection are:

- Asset management (including cyber key terrain)
- Upgrade/patch management
- Vulnerability management
- Vulnerability scanning and system testing
- Heuristic detection and analysis, machine learning, and data analytics
- Organizational and individual training and education to minimize the risk of social engineering (this reduces but does not eliminate the risk)

Traditional approaches to protecting the confidentiality, integrity, and availability of information provide a starting basis for security. However, prevention and basic "cyber hygiene" are not adequate to protect against state threat actors and modern attacks. An Adaptive Defense is a security posture that effectively applies an intelligence and risk-based approach to cybersecurity. Because cyberattacks are inevitable, emphasizing detection rather than prevention will promote more effective security. This approach accepts that the organization may "lose" at the tactical level and be breached; however, quick detection and response will prevent serious harm.

3. Response: Remediation support and the ability to quickly recover from an attack are the essence of an Adaptive Defense. Response should include both the capability to recover quickly from cyberattack and a measurement of the time necessary to resume critical operations after an attack. Response should also include the following sub-domain controls:

- Incident management
- Service continuity management (has a strong dependency on asset identification and management)
- External dependency management
- Internal and external communication
- Stakeholder management

The Response Strategy must among other things establish an incident response coordinator and define protocols that efficiently and effectively inform key stakeholders. These protocols should govern privacy disclosure requirements and assignment of work streams for investigation, remediation, communication, and execution of the response plan.

> “At the heart of the Adaptive Defense is the concept of continuous improvement.

Finally, analysis of “lessons learned” from each attack and response is an important element to guide and adjust intelligence for future responses. Resilience includes learning capabilities. At the heart of the Adaptive Defense is the concept of continuous improvement. This is essential to meet the challenges of emerging and evolving threats. Law enforcement and intelligence services can also be an important partner in effective resilience building.

4. Analysis: Analysis includes containment, forensic investigation and kill chain reconstruction. An effective strategy should emphasize adaptation based on analysis of known attacks. This post-incident analysis forms the basis of an adaptive response by adjusting controls based upon actual known risks. Analysis of known attacks can promote adoption of appropriate technical and organizational measures to safeguard data, systems, and other assets at a security level appropriate to actual risks. This focuses resources on preventing, detecting, and minimizing the impact of known threat methodologies.

Understanding attacker tactics and methods promotes informed decision making, (improved) integration of intelligence, and timely response. Strategic and tactical analysis play an important role in forecasting trends, developments, capabilities, and intentions of attackers, further improving an organization’s Adaptive Defense capabilities.

Figure 1. Illustration of the core elements of Resilience. Source: own compilation

B. Coordination

Adaptive Defense and its main domains should have preventive, reactive, and proactive dimensions. Coordination includes strategies, policies, and activities that further the efficient and effective operation of the cybersecurity strategy across an organization as well as the engagement with external partners.

Strengthened communication between government agencies in cybersecurity matters, between law enforcement and private sector organizations, and between nations plays a central role in increasing the efficiency and effectiveness of responses against cyberattacks.

A foundation for a coordination strategy should include five core areas, as illustrated in Figure 2.

Figure 2. Five areas of action of an Adaptive Defense's coordination strategy. Source: own compilation.

Oversight of the coordination process should be a cross-team collaborative approach led by the organizational Chief Information Security Officer (CISO). Security requires a coordination structure to serve as the support mechanism to guide the program, resolve critical decisions, and establish communication channels. Having cross-functional support greatly helps in developing policy and the organizational changes required to be successful.

C. Capacity

A critical element of capacity building is the ability to incorporate (global) threat intelligence or actionable information into an overall organizational adaptive defense. Given the variety and complexity of information sharing needs, it is impossible to identify a single best threat intelligence sharing model. However, key

elements should be standardization, harmonization, and appropriate aggregation as well as strategic, tactical, and operational capacities to perform analytical tasks based on threat information. Despite the difficulty of coordinating information sharing between the public and private sectors, exchange of information is critical to building capacity across organizations. The ability to use threat information to identify threat indicators saves time, money and quickens response. This is the foundation of establishing and increasing capacity.

Coordination and education are also key elements in establishing and ensuring capacity and cyber resilience. The capacity-building process should identify measures and best practices in support of the core Adaptive Defense domains.

The goal is to adopt a capacity-building approach that leverages internal and external resources to increase organizational capability and facilitate organizational resilience. A critical foundation is to incorporate threat intelligence and incident response planning.

D. Cooperation

The area of public-private partnership, including cooperation with industry partners, the financial sector, academia, and law enforcement, plays an important role in increasing cybersecurity and resilience through raising awareness of threats and preparing adequate support for an effective response. The main areas are:

- Law enforcement partnership (including reporting, prevention, deterrence, disruption, investigation, and victim support)
- Cooperation with third parties, including industry (examples are awareness campaigns, promoting security by design, security by default and privacy by default, and tool development)
- Communication channels for the secure and lawful exchange of information and intelligence with relevant partners

When it comes to detecting and preventing cyberattacks the cliché “it takes a network to defeat a network” is often used. Given the borderless, asymmetric character, volume, level of sophistication, and financial impact of these attacks, cooperation of all stakeholders at national and international levels is key to an Adaptive Defense. This also needs standardised rules of engagement, as well as a clear understanding of the extent to which private parties can obtain evidence themselves and the legal implications of their actions.

CONCLUSION

An Adaptive Defense effectively applies all of the core security domains at a level appropriate to the threats and risk posture of the organization and adjusts strategic decisions based on real-time, global, actionable intelligence. The CMM model provides a framework for evaluating and implementing an Adaptive Defense plan. The CMM process can help create an increased understanding of existing capabilities and an accurate assessment of needs. This provides greater awareness of risks and improves the security readiness process. The development of an information security maturity model requires long-term planning and internal support. It is critical to adopt measures that incorporate emerging best practices into a security framework that will place the organization in a better position to detect and defend against sophisticated cybersecurity threats. An Adaptive Defense is the intended outcome of the CMM process. It is an efficient and effective long-term holistic response to cyber threats. This includes coordinating mechanisms, intelligence sharing systems, and effective policy frameworks leading to a sustainable, agile, and effective risk management security programme. ■

OPINION

WE WANT CUSTOMERS TO TRUST BIOMETRICS

WITOLD SUDOMIR
is the Director of the Department of Safety and Security Technology – responsible for the project entitled "Multimodal biometrics system for identity verification of bank customer". He has participated in major projects concerning: the preparation of the employment and organisational structure to carry out upgrades of technological security systems at nearly 900 bank branches and 550 ATMs, preparation of the assumptions and implementation of the first Polish central system for the monitoring of fire alarms from bank branches, development of regulations in the scope of the safety of persons and property at the Bank, development and implementation of technical protections for bank facilities, and the preparation and implementation of new banking products in the scope of retail and corporate customer service.

One of the major technological challenges faced by banking is related to customers' expectations of fast and secure access to finance. The solution to the dilemma – comfortable or fast and secure – may be biometrics. Its development constitutes an important point in the plans of banking institutions. For biometrics to be successful in banking, equally important as the issues of improving security is to win customer acceptance for new technology in everyday access to finance. This is why we decided to investigate customer attitudes to biometrics as well as the operation of the developed devices at bank branches during standard service processes.

It is true that Poland has been viewed as a precursor and leader in implementing biometric solutions on the "Old Continent." The potential of biometric opportunities has been very measurable, but to employ it effectively, it must be shaped properly and embedded in the reality of everyday life, including the banking reality. For this reason, PKO Bank Polski together with the Gdańsk University of Technology and the Microsystem company based in Sopot addressed the challenge of constructing a complex biometric solution as part of the IDENT research project co-financed by the National Centre for Research and Development. It has been a challenging road from the very idea of biometrics and fascination with its possibilities, through the technologies and solutions that will defend it effectively, to the customer who, by using these solutions, will issue a certificate of biometric confidence to the Bank. Therefore, it seems so crucial and sensible to use a research approach that will enable preparing appropriate solutions based not only on the actual results obtained but also on the expectations of customers.

In the very beginning, when tools and methods were made available (expensive technology due its infancy stage) that enabled the application of biometrics in everyday life, biometric technology was considered as one of the authorisation methods, be it in access control or in transactional systems. Projects were prepared and launched whose purpose was to secure single simple processes. Initially, biometrics was applied enthusiastically in transactional devices to explore the possibilities of replacing cards or the PIN code, thus passing registration to the end user of biometrics. The process related to biometric sampling was not planned, nor were customer needs or ergonomics taken into account. When we view the current solutions that have been implemented at some banks, we notice that they have not represented an attitude to biometrics as a complex tool for customer identification in various service channels, starting from establishing and confirming his or her identity.

The present condition of the implemented biometric solutions is confirmed by the fact that there has been a race to introduce biometric solutions as quickly as possible, not thinking about their ergonomics and trying to achieve customer satisfaction by force. Completely omitted was the aspect of correctly registering the samples at the bank counter, thus passing this important element to the customer at the ATM, which caused many problems during the first registration and contributed to discouragement, and finally abandonment of the new, unknown form of authorisation.

At the same time, a mistake was made in neglecting such a crucial element as social education. The solution was dedicated to small communities with a small range, with a limited knowledge and confidence in the method, precisely due to the lack of publicly available information in that scope. At the same time, the stage of implementing counters for the registration (due to the costs) of biometric data at bank branches was postponed. Every new solution initially finds its enthusiasts which start to use it, but even the greatest amount of enthusiasm will soon fade without relevant mechanisms of sustaining it, as was the case here. The customers, left to themselves, stopped using the solution. The decrease in interest influenced postponing the decision to implement the counters at branches, whereas the customers who dealt with the solution only at ATMs, abandoned it as they were not able to use biometrics in a wider scope, including the bank branches. Over time, the process ceased to be new and to engender enthusiasm; it was not supported by any marketing or product elements and it lost its attractiveness as a consequence.

At PKO Bank Polski, we place emphasis on the security of our customers, their data and transactions as well as on reliable, ergonomic and modern service. Therefore, when considering the need to implement biometrics, we commenced that process by conducting research both into biometric methods and in the needs and feelings of customers regarding a given type of biometrics. Together with consortium members as part of the project entitled "Multimodal biometrics system for identity verification of bank customer", we developed an innovative bank counter based on the new and already known biometric methods. The developed technology enables automatic verification of a bank customer's identity, at the same time offering very high authorisation effectiveness and increasing the comfort of using verification systems on the customer's side. The counter prepared will provide an alternative to the currently implemented simple biometric methods and to the well-known and outdated methods taking advantage of customer knowledge.

In the process of preparing and developing the counter, examined and then implemented will be the following modalities of our own design: an electronic pen analysing the customer's signature in a dynamic manner (while writing), a time-of-flight (ToF) camera supplying information on the customer's facial features, a reader that analyses the distribution of blood vessels in the customer's palm, and a phonic (voice) modality.

The main element of the counter is an innovative smart pen used for sampling the customer's signature in a static and dynamic manner. Static analysis consists in processing the recorded signature image in such a manner as to obtain individual signature features. The extracted static parameters include: the lower contour of the signature, the amount of intersections on the "signature – background" line, and the amount of closed areas in the signature. The dynamic analysis records the signal in the form of a string of samples, whose amount depends on the tablet's sampling rate, i.e. the speed of recording pen movement on the tablet's surface. The recorded signature is treated as a complex signal. To each signature sample, appropriate coordinates are assigned on the complex plane. A signature in such a form is composed of a specific number of samples, depending on the tablet's sampling rate and the duration of writing the signature. In order to record additional parameters, it is necessary to have a special sensor-equipped pen which will capture the above-mentioned parameters as well as

a surface recording the signature, integrated with the pen. The special sensor-equipped pen has been developed by a team from the Multimedia Systems Department at the Gdańsk University of Technology as part of the IDENT project.

The counter has been prepared with the use of an innovative approach to the fusion of biometric characteristics coming from multiple biometric modalities. By using modern encryption methods and not storing sensitive data, the system will increase the safety of confidential information necessary for verification. According to the assumptions, the developed system is expected to decrease the role of an employee in the process of bank customer verification through automatic control carried out depending on the banking transaction performed by the customer. As a result, the waiting time for banking transactions to be performed is reduced. An additional

effect of works on the counter as part of the IDENT project will be developing innovative biometric methods utilising dynamic signature analysis based on a unique pen and laser photogrammetry. The final stage planned in the project schedule will be the pilot implementation of the new authorisation system in 60 branches of PKO Bank Polski, which is scheduled between the first and second quarter of this year.

Areas where biometrics may be applied

The works currently conducted at PKO Bank Polski will allow us in the future to develop services based on biometric solutions in all channels – not only at branches, but also in mobile and online banking. It is also an unavoidable trend in development to introduce biometric authorisation methods to payments. Therefore, the use of biometric methods will enable dispensing with the traditional authorisation methods using PIN codes and passwords.

Biometrics may also be applied in numerous other domains of our everyday life – in healthcare or public administration, for instance. Using it is a chance to improve the comfort and security of services provided to customers, public institutions and patients. Moreover, it is an eco-friendly solution as the amount of paper documents in circulation will be reduced. In public offices alone, 8 million sheets of paper are used every day.

While executing the tasks, we bear in mind the fact that biometrics and related solutions have to provide the customer with a sense of security, freedom of use as well as guarantee the continuity and incontestability of processes to which they are applied.

Every day, humanity develops ever new technologies and an unprecedented miniaturisation of solutions is taking place all the time. It may be expected that this will enable the emergence and application of ever new sensors to enhance the existing biometric methods and develop novel, more advanced solutions.

We must currently focus on the implementation of those biometric methods that are socially acceptable on a wider scale and enable mutual support as well as such methods that will be able to serve multiple channels thanks to their properties. This will also help pave the way for the application of biometrics in other spheres of our everyday life. ■

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

Follow the news @ECJournal

THE ECJ IS ADRESSED TO

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

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

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

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

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

We invite you to follow our initiatives and get involved.

Kraków, Poland.

www.ik.org.pl

THE KOSCIUSZKO INSTITUTE

is the publisher of

EUROPEAN CYBERSECURITY JOURNAL