

EUROPEAN CYBERSECURITY FORUM

The 3rd Annual
Public Policy Conference
dedicated to strategic
aspects of cybersecurity

9-10 OCTOBER 2017
KRAKÓW, POLAND



CYBERSEC

CYBERSEC 2017

RECOMMENDATIONS AND KEY TAKEAWAYS

www.cybersecforum.eu



The conference is co-financed by NATO's Public Diplomacy Division



Ministry of Foreign Affairs
Republic of Poland

Public task co-financed by the Ministry of Foreign Affairs of the Republic of Poland under the Public Diplomacy 2017 competition and the component "The civil and municipal dimension of Poland's foreign policy 2017"



The publication presents the opinions of its authors and cannot be equated with the official position of the Polish Ministry of Foreign Affairs or any of the partners or patrons of the publication.

The publication is available under license Creative Commons Uznanie Autorstwa 3.0 Polska. Some rights are restricted to the Stowarzyszenie Instytut Kościuszki. The content was created under the Public Diplomacy 2017 competition and the component „The civil and municipal dimension of Poland's foreign policy 2017”. It is allowed to use the content under condition of non-disclosure of the above-mentioned information, including information about the license, rights holders and the Public Diplomacy 2017 competition and the component „The civil and municipal dimension of Poland's foreign policy 2017”.

LET'S DEAL WITH CYBER DISRUPTION BY IMPLEMENTING CYBERSEC RECOMMENDATIONS

During over 80 discussion panels, interviews and presentations at CYBERSEC 2017, 150 speakers focused their attention on dealing with cyber disruption. We are extremely grateful to all of them. Subsequently, the CYBERSEC team has selected the key takeaway points, systematised them and grouped them thematically in order to present them to you in the form of recommendations.

Great minds think alike and plenty of our panellists share the same views of digital processes. However, the respective recommendations do not always reflect the statements made by a single person only. In some cases, which are marked with an asterisk (*), additional references to generally available texts and audio-visual aids have been added to facilitate a more in-depth research of a given topic.

We truly hope that these recommendations will inspire all actors playing their part in the digital transformation to engage in intellectual deliberations: decision-makers to take wise decisions when it comes to the development of public policies and business strategies, and technology innovators to take further action for the benefit of sustainable digital growth.

As a warm-up for our cybersecurity considerations, let us start with the number one recommendation:

Closing the gap in the strategic thinking about security is needed. And it is needed NOW.

As a strategic challenge, it requires significant costs. We need to spend money on cybersecurity, but we need to spend it wisely and that should be reflected in the area of procurements.

Higher spending is going to create added value – and procurements that promote security will definitely mobilise producers to create more secure products (also IoT) and services.

Governments must take the lead in the quest for cyber trust.

Therefore, we would like to warmly invite you to attend the next editions of CYBERSEC to build trust and reinforce collaboration.

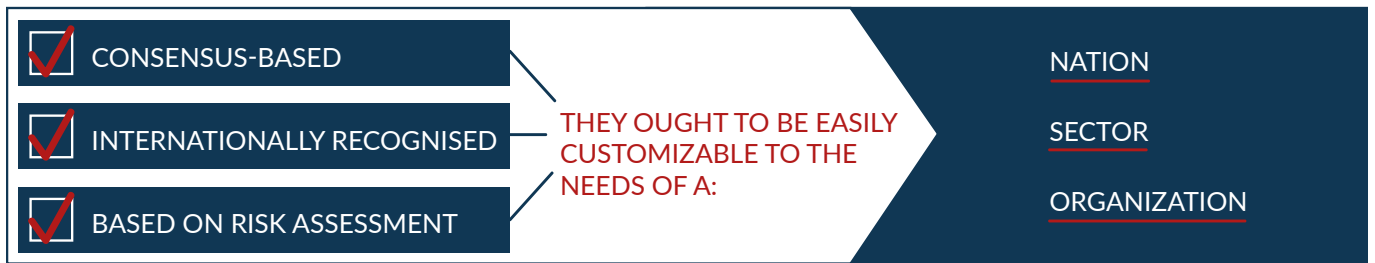
**See you on 27 February in Brussels
and 8-9 October 2018 in Kraków.**

STATE STREAM



THE ROLE OF CYBERSECURITY STANDARDS IN PROTECTING CRITICAL INFRASTRUCTURE

Common standards may strongly contribute to the development of a higher level of cybersecurity, but also help to build the digital single market. To achieve this goal, it is strongly recommended that shared standards are determined, which are:



NOTE: it is proven that sector-specific security standards for critical infrastructure increase vastly the level of cybersecurity.

A mandatory approach in the context of standards should provide for a system of incentives that will help and encourage business to implement them.



Consider creating Mobile Incident Response Teams to provide (only upon request) technical support to CI operators and public authorities in case of a serious, large-scale cyber incident.

COMBATING INFORMATION WARFARE IN CYBERSPACE

A few steps need to be undertaken to secure our liberal-democratic societies against the threats of information warfare conducted in cyberspace:

- We have to develop a countervailing message with the aim of promoting our values.
- We should be very careful with counter measures – there is always a risk of censorship and we should avoid that.
- Other areas that require further debate are impersonation on social media and bots activities.
- Traditional media must practise responsible journalism, also when getting information from cyberspace, particularly social media. Professional associations may play an important role in this area. Given the increasing horizontal information flow, which results from the growth of digital platforms and social media, this should be complemented with the civil society's effort to protect the quality of the public debate, fact-checking, critical thinking and awareness raising campaigns.
- Artificial intelligence meant as algorithm-based big data analytics and its capacity for social manipulation is a concern that must be analysed in the nearest future, considering both the downsides and upsides.
- We need better education. Our society right now needs to think through the education system at large and create a long-term plan with a strong emphasis on new technologies as well as values, critical thinking and media literacy.



[To learn more, watch the VIDEO on CYBERSEC youtube channel](#)

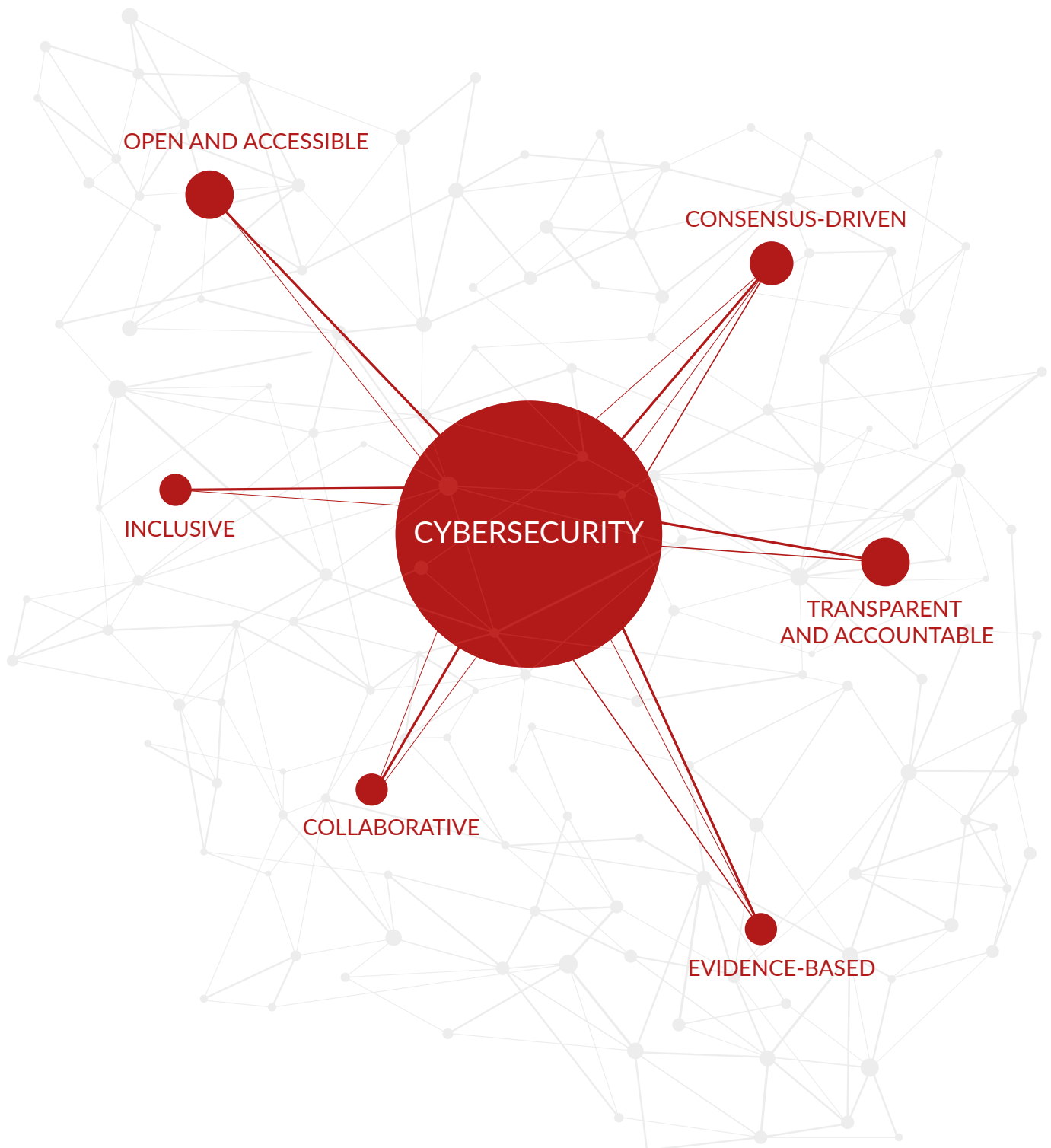
ALL ELECTIONS ARE HACKABLE – BUT IT DOES NOT MEAN WE SHOULD GIVE UP

It would be irresponsible to claim that i-voting is 100 percent secure and that elections systems are unhackable. There is no total security here, just as there are no fully secure traditional election systems. It does not mean, however, that nothing can be done. We need to take holistic actions to address this modern disruption, which will include among others:

- Conducting a comprehensive risk assessment that reaches beyond technology.
- Having the right legal framework in place to make sure that systems have sufficient protection (e.g. recognise i-voting systems as critical infrastructure).
- Providing constant testing, feedback and improvement (to be done by at least two independent parties, also with the use of hackathons).
- Improving cyber hygiene, awareness, capacity-building and operational security of political actors and candidates .
- Introducing transparency measures that build trust and confidence.
- Introducing solid technical measures, such as vote verification (e.g. with the use of separate devices) or traffic monitoring.
- Always keeping an analogue backup version.

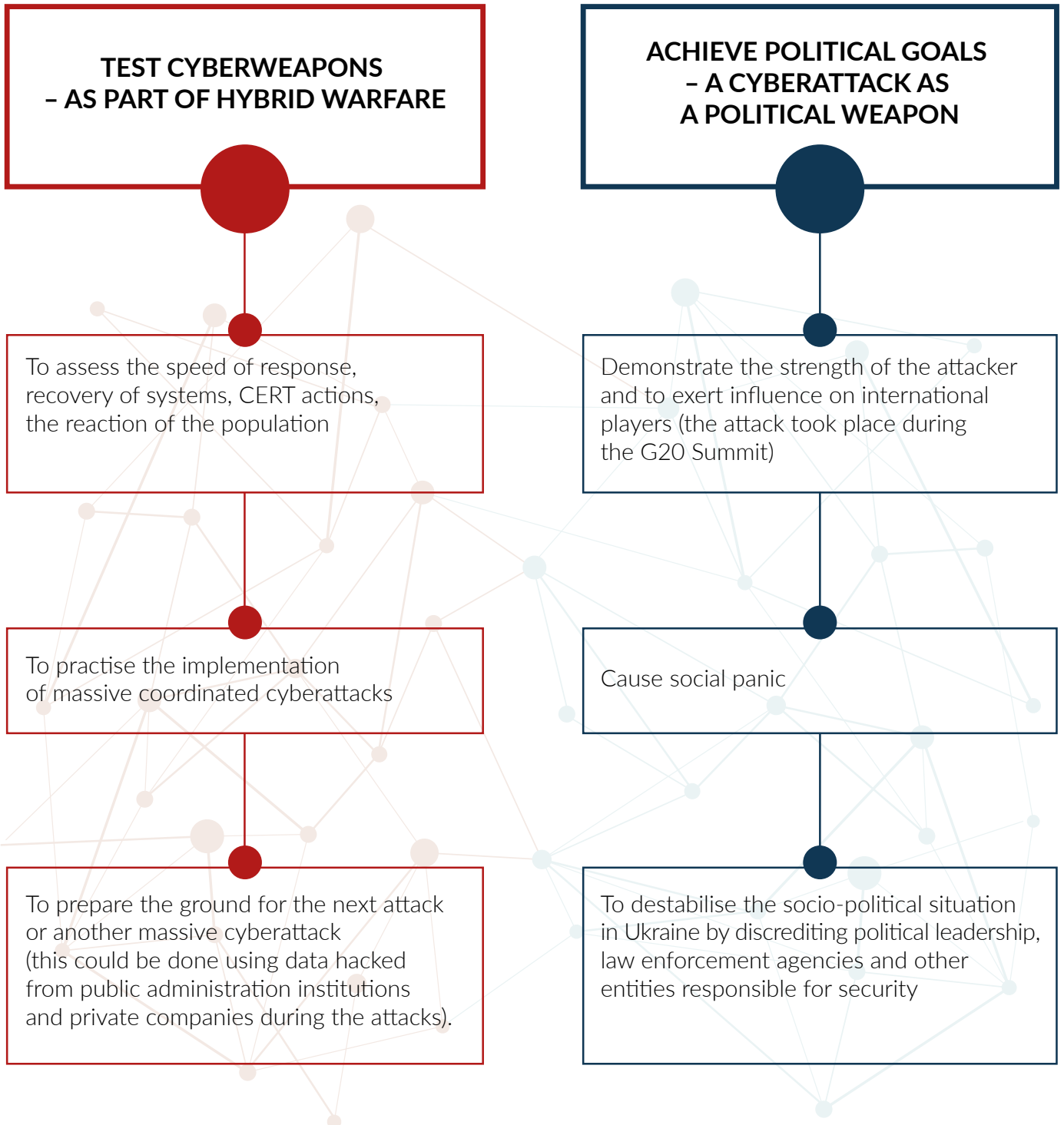
MULTI-STAKEHOLDER APPROACH IN THE AREA OF CYBERSECURITY

There is a very strong need to involve different stakeholders in discussions about cybersecurity. Global Partner Digital distinguishes six main characteristics of a multi-stakeholder approach to policy-making in the area of cybersecurity.



LESSONS LEARNT FROM WANNACRY & PETYA. A UKRAINIAN CASE STUDY

The 'Petya' (also referred to as 'NotPetya') ransomware is a new version of the virus 'WannaCry'. Financial gains and criminal intent are believed to disguise the real motives behind the operation whose real purpose was to:





Stronger cybersecurity engagement and joint actions between the private and the public sector are crucial. Urgent recommendations to be implemented:

- Establish a system of incentives and penalties for companies. Vendors should be incentivised to provide secure products and services.
- Private sector should be encouraged to assist states in strengthening their attribution capabilities.
- It is critical to develop a strong, well-designed vulnerability disclosure policy and update connected devices during their entire lifespan. The private and the public sector must work collaboratively on that.
- A governmental procurement process should require companies to meet certain cybersecurity standards in order to be qualified for government purchasing. For instance 'The Internet of Things Cybersecurity Improvement Act' introduced recently by the U.S. Senate proved that this regulation can increase cybersecurity in a powerful way.
- It is necessary to hold bold discussions on a well-designed system of certification, which may provide useful value from the perspective of cybersecurity, market development and users' awareness. Discussions regarding the appropriate certification model(s) must be conducted with strong participation of strategic, transatlantic allies (mainly from NATO).

INTERNATIONAL COOPERATION OF LAW ENFORCEMENT AUTHORITIES

Law enforcement authorities face multi-faceted challenges when fighting cybercrime:

- Information overload – they need to work with massive amounts of information that cannot be analysed using conventional tools. This is where the help of the private sector and startups is needed. Tools which will help to analyse information and provide foresight are urgently required.
- Workforce shortage – since the public sector often struggles to recruit needed talents, it must start searching for different career models to offer. One option is to introduce short-term contracts in the public environment, with the option to extend collaboration once the person has transferred to the private sector. Workforce as a service is another idea. Outsourcing 'Cyber Task Forces', at least to some extent, might be a solution, too.
- Complicated crime reporting process – cooperation with police and between national police forces will be more effective if the process of reporting crime and fraud is simplified.
- Limited access to electronic evidence – mechanisms that will facilitate cross-border access to electronic evidence are extremely necessary.



DEFENCE STREAM

HOW TO ACHIEVE MISSION ASSURANCE AND STRENGTHEN NATO'S CYBER DEFENCE

In the digital era, the primary focus must be on the goal of mission assurance, which requires:



- Changes to the mind-set – the reasoning that we can rely on systems and the integrity of information in those systems by only investing in skills and capabilities is deeply flawed. The assumption must be that systems are bound to be disrupted and degraded due to the constant threat of cyberattacks, so it is necessary to achieve mission assurance despite that. This way of thinking must be mainstreamed into training, education, planning etc.
- Key stakeholders to focus on identifying vital military assets that are the most critical from the mission assurance point of view, and concentrate on their protection in the first place.
- The key capabilities to be prepared to execute mission assurance in cyberspace – starting with a doctrine, policies, organisation, situation awareness at the NATO level, training, exercising strengthened civil-military synergies, political and legal principles to integrate voluntarily provided national cyber effects and planning mechanisms. To some extent, this has already been implemented in the decisions of the 8 November Defence Ministers meeting of the NAC.
- NATO to bring and implement innovation faster, for example the use of advanced cyber analytics including algorithm-based machine learning.
- Cyberattacks and the cyber threat landscape to be viewed as closely interlinked with other types of attacks, mainly conventional attacks. A cyberattack is sometimes a preliminary to conventional military operations.
- Cyber operations to be considered as a cross-domain capability, in addition to and in support of more conventional operations.



To learn more, watch the VIDEO
on CYBERSEC youtube channel

THE APPLICABILITY OF THE INTERNET OF THINGS TO THE BATTLEFIELD ENVIRONMENT*

Military application of the IoT must be seen from many angles – not only from the combat perspective (where the IoT supports the missions, e.g. logistic, collaborative sensing, automation, acquiring information and diminishing the fog of war, rescue alerts, C2 activities), but also from the perspective of humanitarian assistance and disaster relief. The co-existence and co-deployment of military and commercial IoT systems present many challenges. The three main cyber challenges come down to the following aspects:

SURVIVABILITY	<p>The ability of a system to fulfil its mission in a timely manner despite attacks, failures, or accidents, is the main objective. The concept of survivability differs among civilians and the military. From the civilian perspective, the objective is to make the network survivable. A military system, on the other hand, needs to be survivable in order to achieve its mission target, which means that it needs to take into account disruptive communication (need to address anti-access / area denial communications, asset reallocation / repurposing / redeployment etc.). It needs to respond to disruptions, dislocating resources, relocating assets and devices.</p>	
TRUST	<p>When the military uses commercial IoT devices, the assurance of trust is crucial. Parties must communicate securely and effective identity management is critical. The usage of commercial IoT devices must be based on trusted platform modules which are designed for digital management (they ensure remote attestation, strong group level authentication based on distributed 'Root of Trust for domain', tamper resistance, security of cryptographic material and confidentiality, integrity and authentication of data transmission between network nodes).</p>	
DECENTRALISATION	<p>Decentralised analytic approaches are very relevant for the adoption of the IoT in the military domain. Traditional approaches based on big data analytics solutions running in the cloud have several drawbacks: unacceptably high latency, excessive burden on communications infrastructure etc.) We need to explore fog computing, which is a decentralised communication paradigm – in order to do that, the standard must be created.</p>	

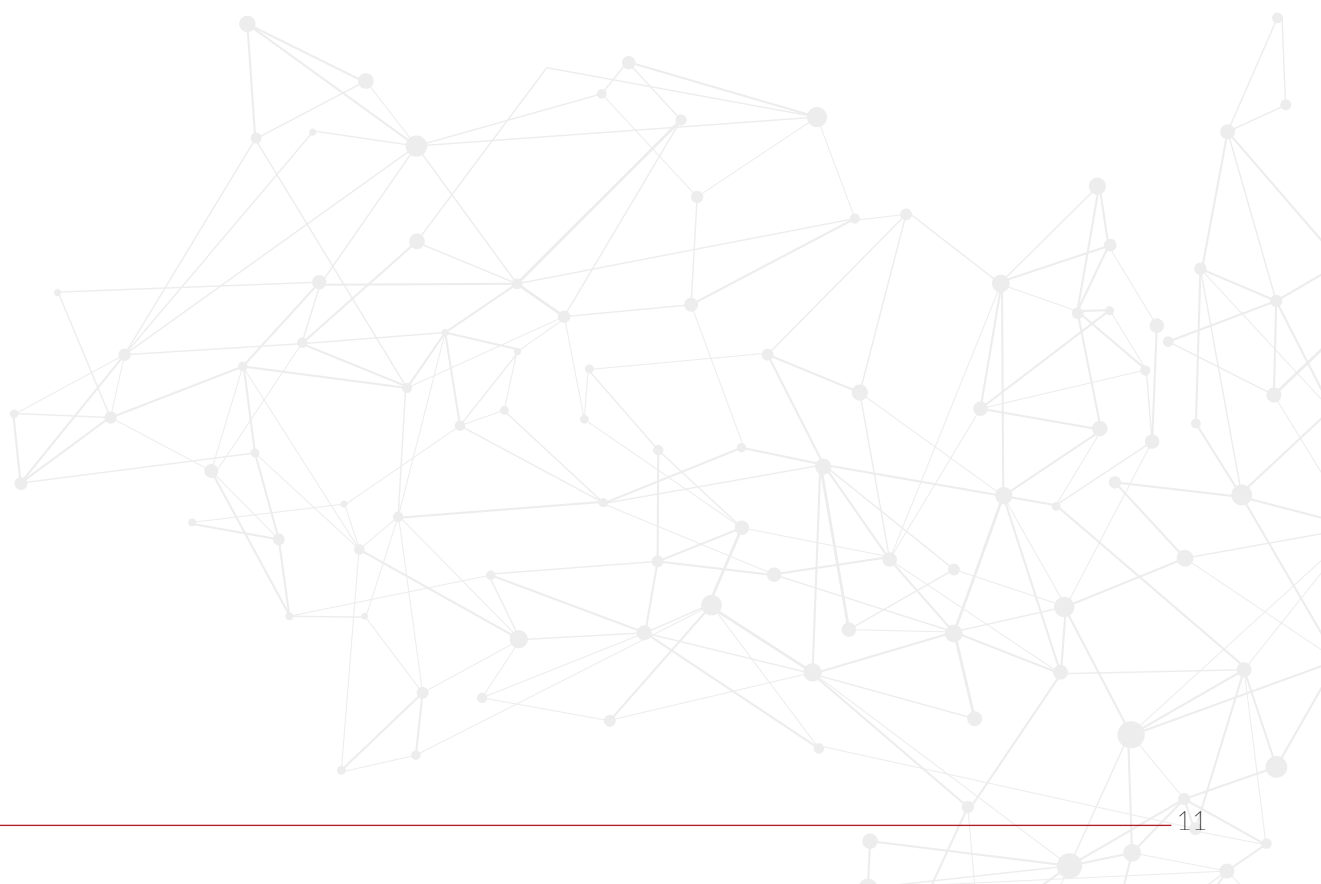
*More on that can be found for instance in the work of Mr Mauro Tortones - Laurel Sadler, James Michaelis, Somiya Metu, Robert Winkler, Niranjan Suri, Anil Raj, and Mauro Tortonesi, A Distributed Value of Information (VoI)-Based Approach for Mission-Adaptive Context-Aware Information Management and Presentation, May 2016

INTERNATIONAL LAW AND CYBER CONFLICTS

We should not assume a priori that a new treaty will resolve all the problems that we currently observe. Development of voluntary cybersecurity norms should be encouraged as an inclusive process involving multiple stakeholders (as many states as possible, but also global non-state actors, such as IOs, NGOs and major IT companies). A global treaty, similar to UN conventions governing the use of the high seas or outer space, should be considered in the future to remove the existing gaps in international law, such as the lack of attribution capabilities resulting in no accountability for cyberattacks. Attribution is a key prerequisite for state responsibility for internationally wrongful acts. Without the ability to establish the linkage between certain cyber occurrences and state actors (government officials, governmental institutions, etc.) inspiring them, the actual masterminds behind such cyber incidents might avoid liability.

While a peace-time legal regime governing cyber activities requires regulation, contemporary norms of the Law of Armed Conflict (LOAC) seem to be relevant and sufficient in terms of regulating cyber warfare. Caution is advised with regards to proposals to introduce new LOAC instruments dedicated exclusively to cyber warfare. The International Committee of the Red Cross as a key stakeholder in this area should definitely be a part of such discussions

- International community accepts that international law applies to cyberspace; the problem is, however, that the understanding of a cyberattack differs among various entities. This is the area that we should work on.
- There are two main criteria international law instruments need to fulfil to properly address cyberspace: flexibility (adaptability) and clarity. This would enhance the possibility for common understanding of how international law applies to and in cyberspace.



FOUR INGREDIENTS OF EFFECTIVE CYBER DETERRENCE

In order to achieve credible deterrence in cyberspace, one must focus on the four main elements:*

1.

ATTRIBUTION: information about the attacker's identity need to be credible. One reason is that a mistake in this area can lead to dangerous consequences. Second, any potential response must be justified in the eyes of others. Taking under consideration the recent events, governments should provide more solid evidence to the public to justify their acts. Third, attribution is a key prerequisite of state responsibility.

2.

THRESHOLD: red lines must be drawn, which when crossed, will lead to retaliation. Thresholds must be clear but flexible at the same time.

3.

CREDIBILITY: retaliation must be credible. Deterrence is as effective as it is going to be assessed and perceived by the aggressor – so communicating capabilities is a key factor.

4.

CAPABILITY: instruments of power used to punish the opponent must be used after careful consideration of consequences. Yet again, they need to be effective against a particular adversary. 'Response-in-kind' will not always be the best option.



To learn more, watch the VIDEO on CYBERSEC youtube channel

*M. Libicki, *It Takes More than Offensive Capability to Have an Effective Cyberdeterrence Posture*, https://www.rand.org/content/dam/rand/pubs/testimonies/CT400/CT465/RAND_CT465.pdf.



Changes in the area of procurements remain critical when it comes to the vital cooperation between the private sector and government. Flexible framework agreements are needed. They should replace firm fixed price, rigid contracts.

Information sharing (with regard to threat intelligence in particular) is pivotal to developing state-of-the-art solutions for customers and enhancing mutual trust.

The defence sector must be ready to improvise, adapt to and overcome challenges. Improving intra-industrial cooperation might be a means to an end.

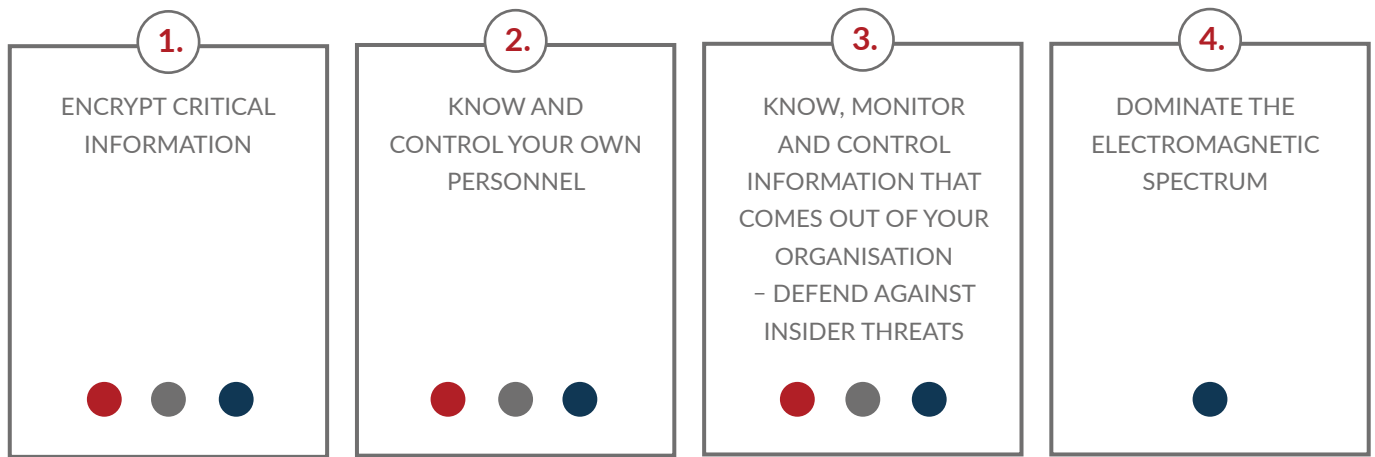
CYBERSPACE OPERATIONS PLANNING – GOOD PRACTICES AND RECOMMENDATIONS

We can distinguish three major types of cyber operations:



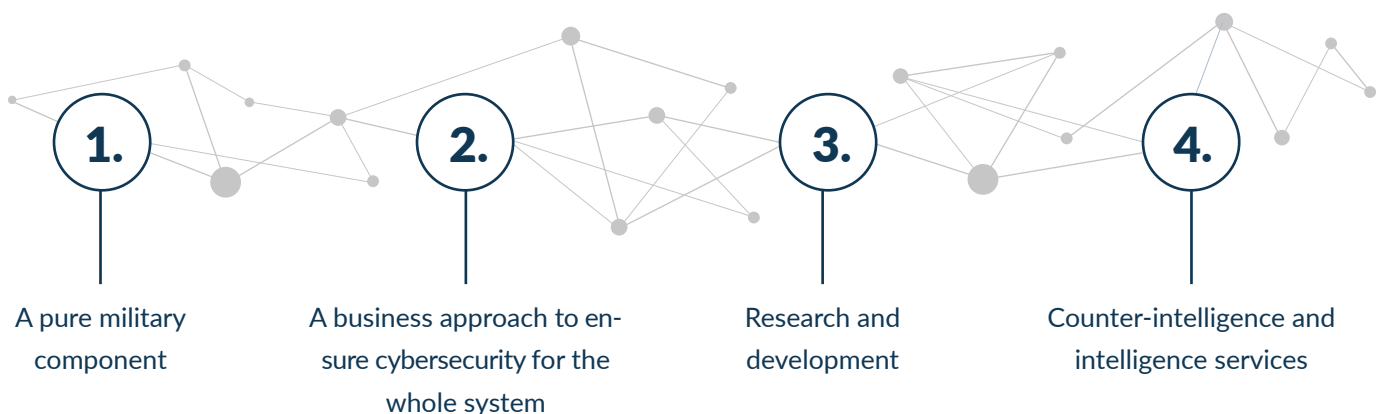
Cyber operations and special operations differ significantly from tactical cyber operations.

There are four main recommendations that should be followed in order to effectively plan cyberspace operations. The first three points are relevant for intelligence cyber operation and the special operations while the **fourth** element is crucial for tactical cyber operations.



POLISH MILITARY CYBER FORCES UNDER CONSTRUCTION

The methodology of capability and organisational structure planning of the Polish armed forces used by the Polish MoD consists of four main areas:



This methodology adopts a capability-based, rather than a resource-based, approach.

FUTURE STREAM



RISK MANAGEMENT IN THE CYBER DOMAIN – TIPS AND TRICKS

- One of the key themes for risk management is to think in a qualitative, not a quantitative manner
- Modern cybersecurity is less and less about blocking tactics. Instead, it is more about answering the question: Who is attacking you? Attribution helps define and better align defensive measures
- Insider threats may be eliminated by developing behavioural analysis. Profiling employees who have access to sensitive information may help detect suspicious behaviour. However, all of those activities must be performed with careful balance against privacy. Consider using red-teaming and controlled social engineering-based 'hacks', e.g. spear-phishing, to enhance employee awareness
- Eliminate silos within security groups

THE SECURITY OF THE CONNECTED WORLD – THE ROLE OF LI-FI

The world is moving toward interconnected autonomous systems where connectivity is one of the most critical elements and one of the most vulnerable parts.

Li-fi provides a fully networked wireless communication technology with features such as the spatial confinement of the light cone that may strongly enhance cybersecurity. In addition, the technology offers the following capabilities:

- It enables very precise localization information to be extracted from the system.
- It allows a thousand times higher data density. That means you could have many devices in close proximity capable of transmitting and receiving data at gigabit speeds.
- It enables a network to be partitioned, so that access is restricted to its certain parts.
- It is immune to jamming or eavesdropping by providing a 'dual gate locking', an additional layer of security based on the specific location of the device that is requesting access to a file.



[To learn more, watch the VIDEO on CYBERSEC youtube channel!](#)

SECURE DEVELOPMENT OF AI

- One of the main threats that must be addressed in the area of AI is bias in algorithms caused by the non-transparency of machine learning algorithms.
- The idea of autonomous weapon systems, 'man out-of-the-loop' systems that are AI-driven is extremely risky due to cybersecurity reasons (e.g. the falsification of signals).
- In relation to the AI usage, the fundamental issue is to assure human liability and accountability. Meaningful human control is essential when AI impacts people's lives.
- Overregulation of AI may ruin innovation; it is not necessary, but accountability, liability and strong basic principles are absolutely essential. The legal boundaries of artificial intelligence need to be agreed globally, not individually at a country level.
- AI is a crucial factor that may resolve problems related to workforce shortage in the cybersecurity area.



To learn more, watch the VIDEO
on CYBERSEC youtube channel

THE ROOTS OF TRUST IN CYBERSECURITY IN THE WORLD OF CONNECTED DEVICES

ENDPOINT DEVICES IN THE FRONT LINE

The cybersecurity of the endpoint devices serves as a backbone of successful IoT revolution. These devices are in the front line of the battle for cybersecurity and it should be our priority to secure them. Every company, public entity and individual user must remember about it.

DECISION THAT CYBERSECURITY IS STRATEGIC CHALLENGE REQUIRES DECISIVE ACTION

Closing the gap in the strategic thinking about security is needed. It is a strategic challenge and it requires significant costs. It must be reflected in the area of procurement. We need to spend money on cybersecurity.

Higher spending is going to create added value – procurements that promote security will definitely mobilise producers to create more secure products (also IoT) and services. Governments must set an example.



To learn more, watch the VIDEO
on CYBERSEC youtube channel

CYBERSECURITY OF SMART CITIES

- The complex landscape of IT and cybersecurity vendors using various products within one ecosystem makes it harder to ensure cybersecurity. This issue requires further consideration.
- It is important to have rules imposing that people can have access to resources and information relevant from the point of view of their responsibilities. Relevant laws and policies must be in place to allow that; however, they will not be able to replace threat awareness and the norms of responsible and reasonable behaviour.
- Public data collected in smart cities must be 'given back' to citizens, so they can use them for various processes, beneficial from the societal and economic point of view. Of course, this must be done in a secure and responsible fashion.
- When developing smart cities, international funds for megatrends (coming from the UN, the World Bank) should be utilised more broadly.
- Public institutions ought to be obliged to publish 'the state of play' with regard to cybersecurity in the cities.

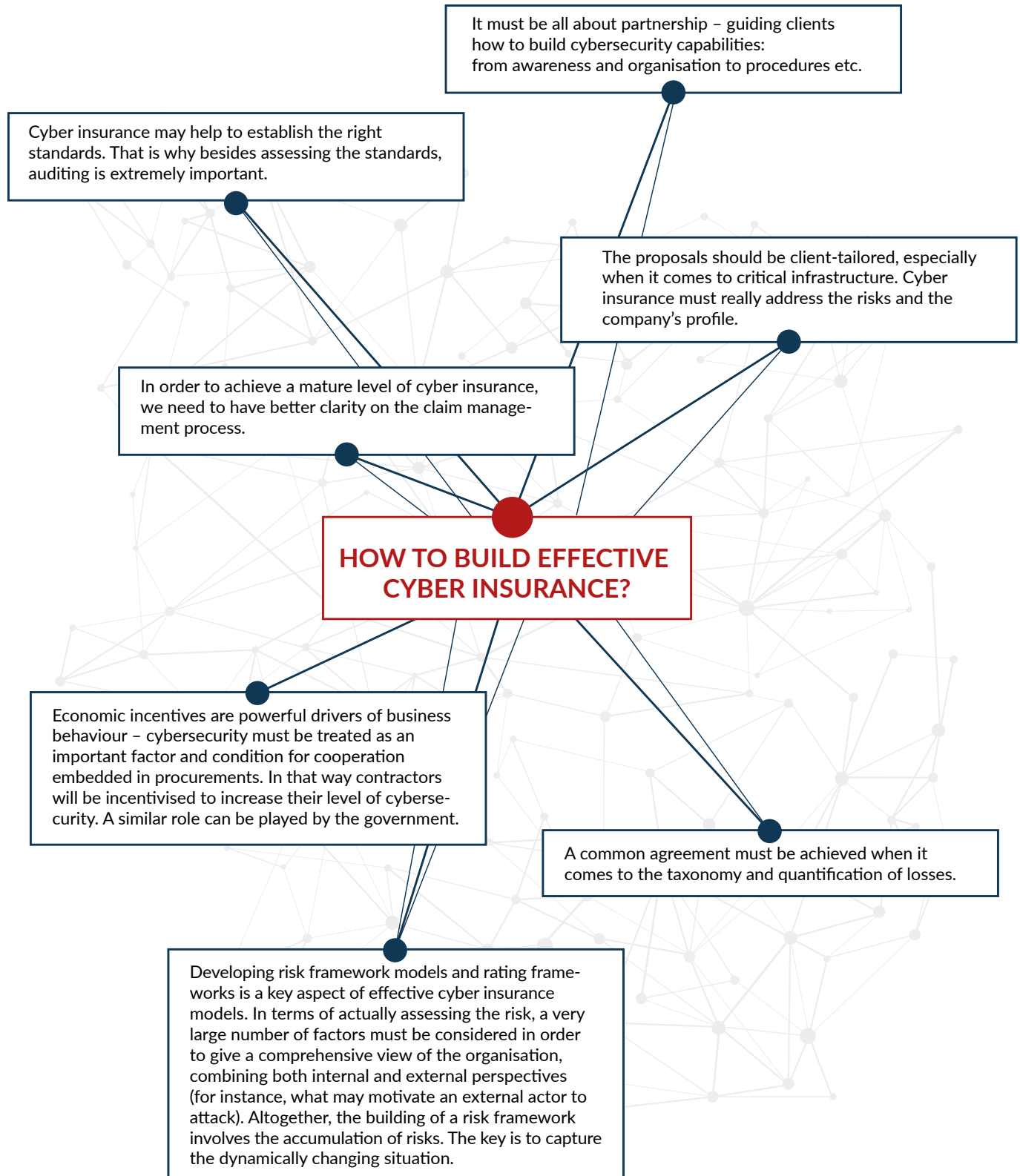


PRIVACY

- We need to agree globally to reduce the amounts of data that are being collected.
- Data security and privacy protection must be treated as a key responsibility when building smart cities. Information must be encrypted and anonymised.
- We have not yet fully appreciated what it means to lose control over information, which, in effect, could be tantamount to the loss of freedom. Privacy is in a way an enabler of democratic rights and values and processes that we want to protect.

CYBER INSURANCE

Providing effective cyber insurance is much more than simply insuring – it is about building cyber risk governance with a strong component of the whole culture around cybersecurity.



To learn more, watch the VIDEO on CYBERCEC youtube channel

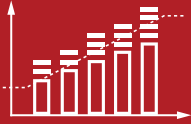
ENHANCING INNOVATION THROUGH REGIONAL CYBERSECURITY ECOSYSTEMS

Cybersecurity is a global challenge which has to be tackled both globally and locally. Building regional ecosystems enables strong and efficient cooperation between different stakeholders.

- A well-functioning ecosystem is based on a triple helix of university, industry, and government. Gathering academic researchers, business and human capital to support innovation cybersecurity centres is not enough. What is required is to create a proper interplay between them and the government, considering the specific nature of each player.
- The needs and challenges of ecosystem parties are different but complement one another:
 - Academia should equip students with practical knowledge, making sure they can contribute to the development of the industry. Team leaders in the industry, developers should be allowed to teach at universities, which would guarantee that academic education goes hand in hand with the latest advances in technology, making students well prepared to enter the labour market. The partnership between the industry and academia can enhance the operation of the entire ecosystem.
 - Cooperation between large corporate players and SMEs in an ecosystem can be challenging. Not always can SMEs, especially startups, guarantee the stability and a long-term partnership yielding a certain level of revenue that large corporations may require. What can help to overcome this problem is to implement the so-called 'umbrella' projects under SMEs and support them during the process of their development. This solution will be mutually beneficial as big companies will increase their innovativeness in return.
 - Government should recognise the potential of selected regional cybersecurity centres and develop special funds to support both educational as well as innovative projects in those specific regions.
- Ecosystems should cooperate internationally in order to learn from one another. Each system is unique and approaches the field of cybersecurity from a different angle. Therefore, the exchange of good practices enables solving different problems in manifold ways. The Global EPIC initiative launched during CYBERSEC 2017 is a perfect example of a platform that facilitates a conscious attempt to '**glocalize**' – localize the global and globalize the local.



To learn more, watch the VIDEO on CYBERSEC youtube channel



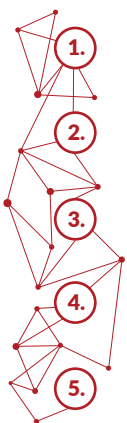
BUSINESS STREAM

THE APPROACH TO CYBERSECURITY IN BUSINESS – ADVICE FROM A TELCO COMPANY

- The entity must take a holistic look at the architecture of the internal network and external connections.
- The OSI mode should be applied, which involves the application level, the network level and data processing.
- Incident management must be in place – detection, response, recovery and protection must be harmonised with the following three pillars: people, processes and technology.
- A system should be designed in such a way that the functionality goes hand in hand with security.
- Risk aware users – everybody who is a user of IT systems must be educated about the dangers in the network and act accordingly to the risks.
- The life cycle of systems – the security of systems must be ensured throughout the whole life of the system.

FUTURE OF THE HEALTH SECTOR

There are five main weaknesses affecting cybersecurity in the health sector:



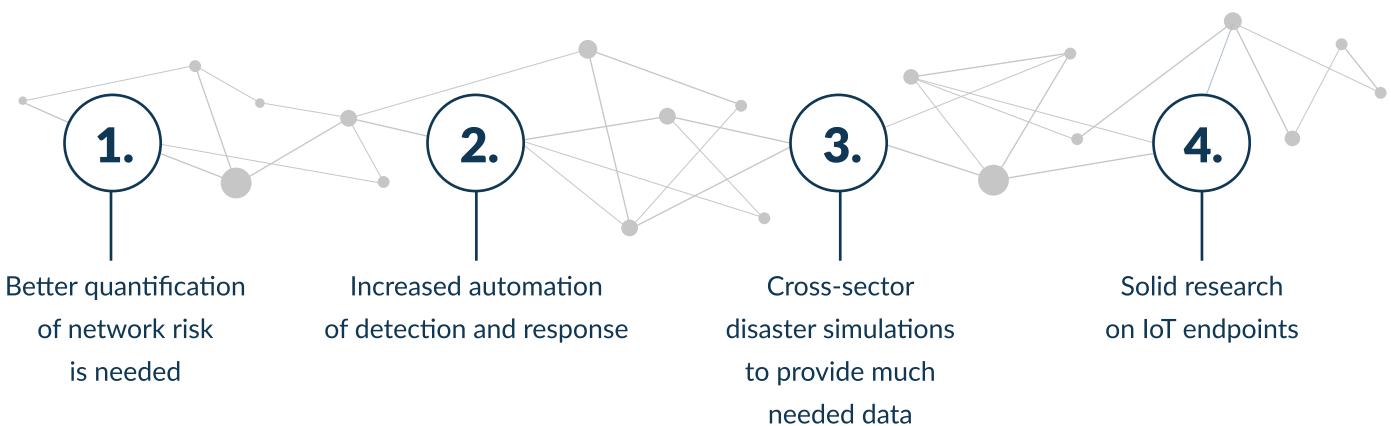
1. A severe lack of talents.
 2. Old, unsupported systems still running critical elements.
 3. The rush to premature over-connectedness which strongly increases risks and threats.
 4. A single point of failure – a single device that fails can bring an entire hospital to a standstill.
 5. Very vulnerable devices.
- In the context of significant workforce shortages, the implementation of cloud-based solutions may have plenty of positive effects: homogenised, more consistent and predictable environment may leave less operational variants and configurational mistakes.
 - The discussion about the future of cybersecurity in the health sector requires bold vision, including a debate on the healthnet – an industry-dedicated network separated from the Internet.
 - Governments should incentivise innovations in the health sector.

TOWARD MORE SECURE NETWORKS FOR CRITICAL SECTORS

Main recommendations:*

- Key controls of operational technology must be isolated from public networks if they are going to be made reasonably secure
- The incentives for security in our societies are widely misaligned – that needs to be fixed by market opportunities, tax policy, liability, regulation – these are the fundamental directions of change

Four research challenges which need to be tackled:



*MIT Center for International Studies, MIT Internet Policy Research Initiative, Keeping America Safe: Toward More Secure Networks For Critical Sectors, <https://internetpolicy.mit.edu/reports/Report-IPRI-CIS-CriticalInfrastructure-2017-Brenner.pdf>



To learn more, watch the VIDEO on CYBERSEC youtube channel

WHY ORGANISATIONS MAY WANT TO SET UP A SECURITY OPERATIONS CENTRE (SOC)?

Effective SOC's increase organisation, improve visibility, prepare us for cyberattacks, as well as enable faster detection and more comprehensive incident response.

How to establish a SOC?

- At least a few components are needed: SIM, good analytics, threat intelligence.
- Cybersecurity requires substantial investment – for instance a well-designed SOC should comprise a minimum of 15 people, three lines, 24/7 monitoring, people with strong capabilities (for example, to react quickly, analyse source code, develop solutions, make a reverse engineering, browse the Dark Net).
- Automation and a holistic approach ought to help with the above-mentioned processes.



To learn more, watch the VIDEO on CYBERSEC youtube channel



CYBERSEC 2017

IN NUMBERS



1
Emerging Public
Policy Challenge



2
Days of Thought
Provoking Debates



4
Thematic
Streams



>600
Articles
about CYBERSEC



>90
Accredited
Journalists



>100K
Twitter
Impressions



1,2 MLN
EUR Advertising
Value Equivalent



>150
Speakers



>220
Individual companies
represented

15%
Academy
& NGO



50%
Private
Sector



35%
Public Administration
& Uniformed Services

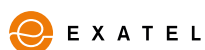
LEARN MORE ABOUT @CYBERSECEU:



STRATEGIC PARTNERS



MAIN PARTNERS



PARTNERS



INNOVATION STAGE PARTNERS



SUPPORTING PARTNERS



LOGISTICS PARTNER



ORGANIZER



HONORARY PATRONS



INSTITUTIONAL PARTNERS



MEDIA PARTNERS



SAVE THE DATE

4th European Cybersecurity Forum CYBERSEC 2018



CYBERSEC

EUROPEAN
CYBERSECURITY FORUM

Brussels
27.
02. DEALING WITH
2018 CYBER DISRUPTION
BRUSSELS LEADERS' FORESIGHT

Kraków
8-9.
10. THE QUEST
2018 FOR CYBER TRUST

WWW.CYBERSECFORUM.EU



[@CYBERSECEU](https://twitter.com/CYBERSECEU)



[/CYBERSECEU](https://www.facebook.com/CYBERSECEU)