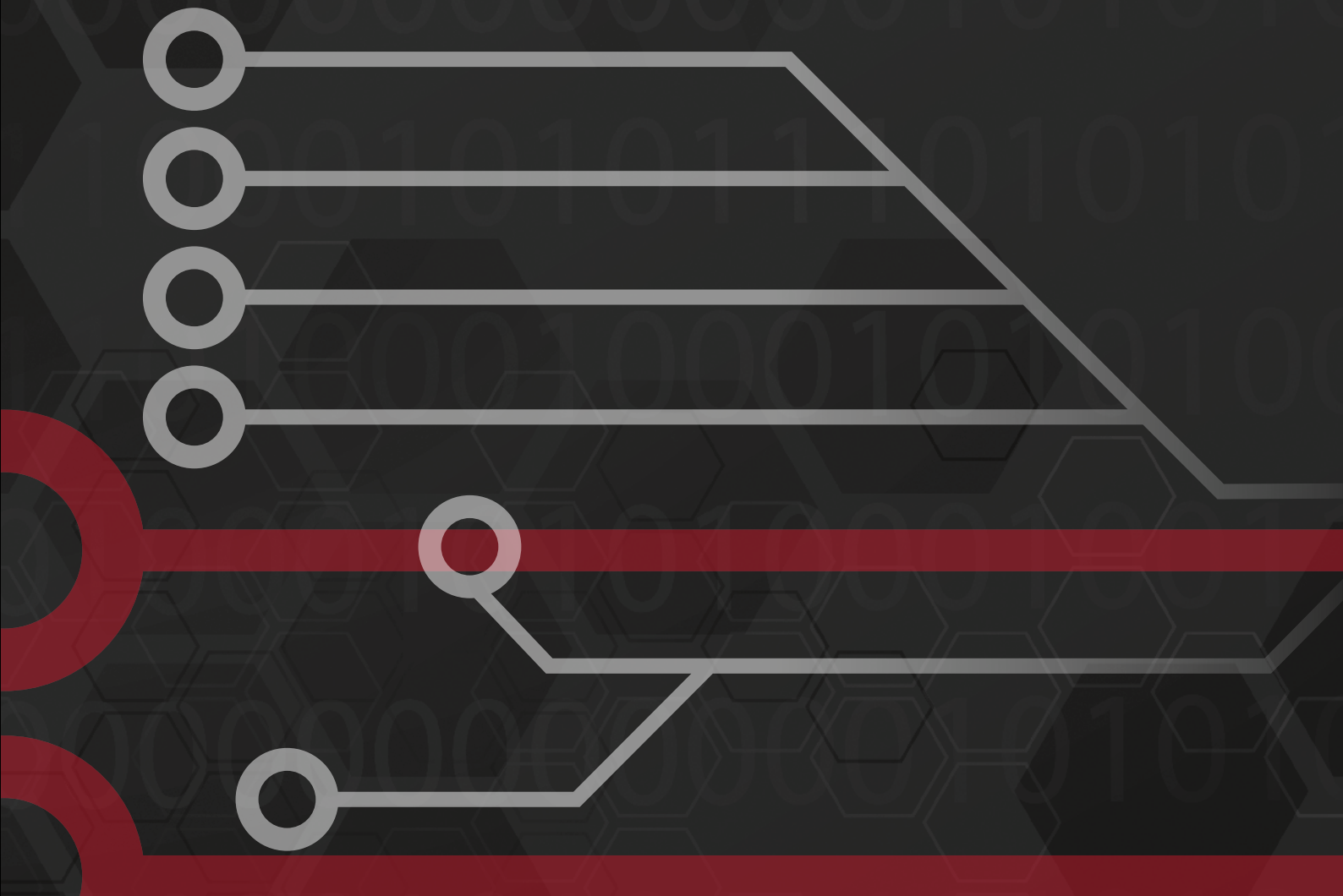
VOLUME 3 (2018) ▪ ISSUE 4

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 (2018), Issue 4, 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

EDITORIAL

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

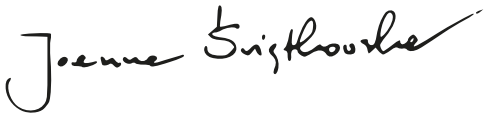
The very first issue of European Cybersecurity Journal in 2018 touches upon topics and problems that will largely determine the course of cybersecurity discussions in the coming months.

At the end of 2017, we asked prominent CYBSERSEC community experts representing different countries and industries what cybersecurity topics will rise to the top of the global agenda in the near future. We were able to collect many responses which revealed some underlying themes and issues showing possible trends. I encourage you to read these predictions as they can help us prepare for events that may materialise very soon. Increased cyberattacks on critical infrastructure or a growing tendency for individual countries to pursue offensive operations are only some of the points on our list.

Many of the already identified themes are elaborated on in this issue of ECJ. I particularly encourage you to read the interviews with Paul Cornish and Paul Timmers, with whom we talk about a number of extremely important aspects related, for instance, to the European cybersecurity policy.

This issue of ECJ also includes recommendations that were developed following the 3rd European Cybersecurity Forum, which took place in October 2017 in Krakow. CYBERSEC 2017 brought together a record-breaking number of 150 speakers and more than 1,000 delegates from all over the world. Among them were policy-makers, top industry experts, global private sector leaders, investors, and technology start-ups. During two days of intensive debates, they came up with a number of best practices and tips, which will certainly contribute to reinforcing many aspects related to the different areas of cybersecurity.

I truly hope they will prove useful and become an inspiration for our readers.



CONTENTS

5 INTERVIEW WITH DR PAUL TIMMERS

9 FINDING A DEFENSIBLE THRESHOLD TO ACHIEVE DETTERENCE IN CYBERSPACE
Professor Martin Libicki

16 A BALANCE OF POWER IN CYBERSPACE
Dr. Alexander Klimburg, Louk Faesen

32 INTERVIEW WITH PROFESSOR PAUL CORNISH

36 LET'S DEAL WITH CYBER DISRUPTION BY IMPLEMENTING CYBERSEC RECOMMENDATIONS

52 WHY SHOULD THE WEST NOT NEGLECT CYBERSECURITY AND INTERNET GOVERNANCE IN CENTRAL ASIA – A BRIEF CASE STUDY OF THE REPUBLIC OF UZBEKISTAN
Magdalena Szwiec

56 INTERVIEW WITH GRZEGORZ JASIULEWICZ

INTERVIEW WITH DR PAUL TIMMERS


© Michael Chia

DR PAUL TIMMERS
is a visiting fellow at Oxford University in cybersecurity. He is a former Director at the European Commission for Digital Society, Trust & Cybersecurity, responsible for policy, legislation and innovation in cybersecurity, digital privacy, digital health & ageing, e government, and smart cities/ mobility/energy. He was member of the Cabinet of European Commissioner Liikanen. He held various academic positions and recently worked with UC Berkeley on cybersecurity. He is also senior advisor at the European Policy Centre in Brussels and investor in digital innovation.

He was manager in a large ICT company and co-founder of an ICT start-up, holds a PhD in physics from Nijmegen University in the Netherlands, an MBA from Warwick University in the UK, was awarded an EU fellowship at UNC Chapel Hill and completed executive cybersecurity education at Harvard.

The recently proposed set of cybersecurity initiatives known as the 'cybersecurity package' underlines the need for 'European strategic autonomy'. Could you please explain what it really means and what the potential benefits are?

The lead paper of the cyber package is the Joint Communication 'Resilience, Deterrence and Defence: Building strong cybersecurity for the EU' released on 13 September 2017. It uses the term 'strategic autonomy' in conjunction with the 'Single Market' and technological capabilities and skills, and states that '[i]t is in the EU's strategic interest to ensure that the EU retains and develops the essential capacities to secure its digital economy, society and democracy, to protect critical hardware and software and to provide key cybersecurity services.'[1] Another context in which 'strategic autonomy' is used is the 2013 EU defence policy. None of these documents, however, defines the term.

It seems reasonable, however, to include in strategic autonomy – in the context of cybersecurity – all these aspects. So let's give it an attempt and define that 'strategic autonomy means having an acceptable level of control over essential elements of the own longer-term future, including economy, society and democracy'. Obviously, there is no such control if major economic activity gets disrupted for a longer period of time or made impossible (e.g. through attacks, IP theft, or extortion). Strategic autonomy is supposed to counter such risks.

Using the word 'acceptable' in this definition already shows a couple of things: first, there is a subjective dimension to it (which is debated in the balance of roles between the EU and the constituent states); and second, that an acceptable level is not necessarily the same as full control. This suggests there may be several ways to achieve an acceptable level of control. Here are five of those:

(1) DIY – do the essential work yourself
(2) Work as trusted partners, e.g. bilaterally or together as the EU countries
(3) Have a trusted third party for validation and/or certification
(4) Use a technological approach like the containment of vulnerabilities or full transparency through an open source approach
(5) Make it politically larger than 'cyber' by bringing in other strategic dependencies like a shared interest in avoiding trade war or kinetic war.

[1] JOIN (2017) 450, Communication 'Resilience, Deterrence and Defence: Building strong cybersecurity for the EU', European Commission, 13 Sept 2017.

The cyber package alludes at least to the elements of (1) – it recognises that Europe needs to hold specific technologies like encryption in its own hands; (2) – it calls for joined-up competence networking and capacity building; (3) – it proposes verifiable and legally supported certification, though it is not clear how this would extend to international supply chain partners (and this is of course a key aspect!); and (5) – by calling for international dialogue on norms and values and including cybersecurity in PESCO, and linking civil and military cybersecurity.

Nevertheless, there is still a lot of work to be done. Commissioner Julian King, when I asked him, called upon academics to also do their part by discussing a definition of strategic autonomy such as the one mentioned above and – most importantly – by reflecting on the modalities of achieving strategic autonomy for example along the five approaches above.

In one of your papers you write that 'there is no EU cybersecurity industrial policy as such'. Is it something that will change in the future, especially that most of the current governments put Industry 4.0 on the top of their political and economic agendas?

What we see today is a range of cyber policy measures that have an industrially relevant dimension – even if they have arisen from another motivation, most notably from the Single Market legal basis. Such measures include certification, the EU's R&I investment and skills. The underpinning standardisation can come from the NIS Directive, which itself is Single Market-based and not at all primarily motivated by industrial policy objectives. These measures can be seen as the constituting elements of a cyber-industrial policy, but together do not represent a full policy palette. They have also not been formulated under an overall industrial policy vision.

Nevertheless, as I have analysed elsewhere, over the years there has been undoubtedly a move towards a stronger set of industrial policy measures as well as an increasing alignment in time and topics in the thinking of the industry and in the thinking of the EU policy circles. In addition, as pointed out rightly in the question, cybersecurity is also part of policies with strong industrial objectives, such as Industry 4.0.

More generally, there has also been over time a gradual re-appraisal and re-instatement of industrial policy in Europe. While the term 'industrial policy' was perhaps shunned some 15 years ago, since 2005, it has gradually come back into the policy debate and been re-legitimised[2]. A clear example of that is the recent publication of a UK industrial policy. An example at the EU level is a 'renewed industrial policy' that the Commission tabled in September 2017, at the same time as the cyber package (!), after a request by the Council in May 2017. In the meantime, the Council in its Conclusions adopted on 1 December 2017 asked the Commission to do even more namely to 'further develop a comprehensive EU industrial strategy with a focus on 2030'.

I think it is safe to say that the EU clearly aims to be a competitive player in the global cybersecurity market. Undoubtedly, it is going to be a great challenge given the position of other players. How to beef up the EU's position? Do you have any advice here?

This is a huge challenge indeed, and it starts with the budget that we set for cybersecurity in Europe which may be 5-10 times smaller than the budget of the US or China. Clearly, the willingness to put money into operational and longer-term (R&I) cybersecurity has to increase in the Member States and at the European level. The current EU multi-annual framework budget discussions must be an entry point for that, and the Commission already made some suggestions in that regard in the September 2017 cyber package.

Even if more money is found, we will, however, have to be using it in smart(er) ways by:
(1) Focusing and being selective in what we spend on
(2) Seeking synergies between cybersecurity and other investment areas like Industry 4.0, self-driving and connected cars, smart energy, digital health etc., but also combining strong cybersecurity with our strength in data protection (based on the GDPR) to become a more competitive global player, and
(3) Entering into key partnerships with other world players.

[2] See for example Jacques Pelkmans, 'European Industrial Policy', in International Handbook on Industrial Policy 2006, eds Patrizio Bianchi & Sandrine Labory, pp. 45-78.

Points (1) and (3) above directly relate to the discussion on strategic autonomy and can benefit from point (2). To illustrate this with an example: we would like to see smart transport as an essential element of our longer-term economic and social future, so it is a part of strategic autonomy. But even if we do not control the complete supply chain of smart cars, we can focus on providing key components and activities such as assembly, including security-related components and activities, and combine those with contributions from third countries. The joint interest would be open, unhampered trade. Such a combination of focus, synergies, and a degree of partnership will require common norms among the states to be established. It will not work if one of the parties considers a smart car a weapon. So there is still work to be done in the area of an international cyberspace policy as well.

Recently, we have learned that EU governments agreed upon the message that cyberattacks can be an act of war. It seems to be an important element of a new deterrence posture. But deterrence is efficient only if combined with reliable attribution. What are the most important capacities that we, the EU and its Member States, should build in this area?

Without claiming to have the knowledge to be able to say much about this, for sure information sharing is essential – just as intelligence sharing is. Information sharing is indeed foreseen at the EU level in the NIS Directive as well as in cooperation between judicial and police authorities. The cyber package extends this with a Recommendation on a 'Coordinated Response to Large Scale Cybersecurity Incidents and Crises', which connects the technical, operational, public communications, strategic and political levels. Indirectly, it also states that it should help identify the causes of incidents.

One may ask: What about cross-sector information sharing and cyber incident handling? Are those sufficiently provided for? In principle, the mechanisms exist, but they are minimal; they need to be profoundly exercised and such cyber-exercises are to be regular and frequent. This is also likely to help make attribution firmer. One of the big risks in cyber deterrence based on uncertain attribution is that active defence may miss the target or hit the wrong target. A crucial question is then: How will deterrence actually work? What about the risk of uncontrolled escalation? Academics like Oxford's Lucas Kello in his book 'The Virtual Weapon' are talking of punctuated deterrence with cumulative effects (accretional principle).

We often hear that ensuring cybersecurity is a global challenge and you need to cooperate internationally, especially with like-minded partners. It seems natural to deepen transatlantic cooperation, but in which direction should we develop this particular partnership? Any proposals for other joint initiatives?

Actually, it may not be an insurmountable challenge to define an international agenda, or at least a transatlantic one. It may be more difficult to find governance for such an agenda, certainly at the time when forums led by multi-lateral governments seem to get weakened. UCSD's Cowhey and Aronson in their book 'Digital DNA' are making a plea for multi-stakeholder approaches, new ones or existing ones, that would incorporate cybersecurity into their agendas. That may make a lot of sense. For example, consider the automotive sector which has a pressing need to address cybersecurity and whose governance is largely industry-led with a degree of government involvement and some civil society involvement.

As for the agenda itself, I would say we should start with awareness, skills and knowledge building. A lot of bilateral work is happening already, for example between the U.S. Department of Homeland Security and ministries in several countries as well as in the existing EU–US cyber dialogue and cybersecurity and cybercrime working group. There is a clear common interest given the enormous scarcity of skilled people. We would also continue the work that has already been ongoing on the risk management requirements (as part of the NIS Platform), definitions and classification (see also the work done by the U.S. NIST).

Then, we can start considering the more difficult topic of standards for the agenda. Certainly, certification, including procedures and levels of assurance, is more challenging. But there, too, is a history of mutual recognition based on the Common Criteria.

Perhaps this will also provide a wider access to expensive testing facilities on both sides of the Atlantic. The going will get tough when we talk about encryption and international cyber exercises, let alone the WTO's work on technical barriers to trade discussions. We should not be naïve and over-optimistic, certainly not in the current political climate and the high sensitivities around national security. But it is not an impossible path to walk.

We talked at length about political initiatives, but the last question is about technology. Do you see any chance that new technologies such as blockchain, AI or quantum computing may help to solve problems related to cybersecurity? In other words, can technology be the answer to problems caused by technology in the first place?

In my view, the jury is out on the new technologies. Blockchain looks like a good candidate for trusted validation, which may be useful for certification of devices and possibly of larger systems, too. AI is already being applied to predict and be ahead of botnet attacks as well as to detect infections in individual computer systems more accurately than any human can do.

Quantum mechanics in cybersecurity has two faces: one is quantum entanglement that can be used for quantum communications which cannot be intercepted without being detected, offering highly secure communications; the other is quantum computing which can be used to break today's encryption, potentially making all our past and current communications publicly exposed. What is therefore being researched is post-quantum cryptography which could protect against quantum computing. In any event, politicians agree that Europe cannot afford to be left behind in the quantum and AI developments.

In the meantime, in terms of research and innovation at a European level, quite a lot of action has been taken to raise the budget (though still relatively low) and to notably make a better use of the budget available in the EU's R&D programme Horizon 2020 with the help of more strategic guidance which is developed together with industry. In 2016, industry formed a large collaboration platform, the European Cybersecurity Organisation (ECSO) that has taken the responsibility for partnering on this aspect with the European Commission. ■

Note: Opinions expressed are personal views and cannot be taken to represent the views of the European Commission or the University of Oxford.

Questions by Dr Joanna Świątkowska

ANALYSIS

FINDING A DEFENSIBLE THRESHOLD TO ACHIEVE DETTERENCE IN CYBERSPACE

MARTIN LIBICKI
is an Adjunct Management Scientist at the RAND Corporation, Professor at the Pardee RAND Graduate School, Distinguished Visiting Professor at the U.S. Naval Academy.
Professor Libicki (Ph.D., U.C. Berkeley 1978) holds the Keyser Chair of cybersecurity studies at the U.S. Naval Academy. In addition to teaching, he carries out research in cyberwar and the general impact of information technology on domestic and national security. He is the author of a 2016 textbook on cyberwar, Cyberspace in Peace and War, as well as two others commercially published books, Conquest in Cyberspace: National Security and Information Warfare, and Information Technology Standards: Quest for the Common Byte. He is also the author of numerous RAND monographs, notably Defender's Dilemma, Brandishing Cyberattack Capabilities, Crisis and Escalation in Cyberspace, Global Demographic Change and its Implications for Military Power, Cyberdeterrence and Cyberwar, How Insurgencies End (with Ben Connable), and How Terrorist Groups End (with Seth Jones). Prior employment includes 12 years at the National Defense University, three years on the Navy Staff as program sponsor for industrial preparedness, and three years for the GAO.

The basic theory of deterrence says: 'If you do this, I will do that. If you do something that crosses my red line, I am going to punish you.' But if we get back to this formulation, it turns out that it can be reduced to just four words, each of which has its own importance. The first one is 'You', the second one is 'This', the third one is 'I will', and the fourth one is 'That'. All those four elements have to be thought through before we can say that we have a deterrence policy in place. Admiral Rogers, the head of the U.S. Cyber Command, was fairly straightforward in what he was asking for, when telling Congress that if the U.S. government wanted deterrence, he was going to need a bigger "belt" to use on its opponents. However, it turns out that it is more complicated than that. So, let's take a look at the four basic elements.

The first word is 'You'. If you are going to punish somebody for doing something in cyberspace that crosses your line, you have to have some notion of who they are. You need attribution. Otherwise, how would you know who to punish? During the nuclear era that wasn't a problem. In a bipolar world, it was always the other party who you had to deter. But in cyberspace, there are many capable adversaries: nation-states, organised crime groups, individuals, or even high-schoolers. In order for a nation-state to know who to punish, they have to know where they came from. Ten or fifteen years ago, it was widely believed that in cyberspace "nobody knew you're a dog". In other words, you couldn't tell one person from another in cyberspace. Understanding that attribution was going to be a shortfall and an obstacle to having a deterrence

policy, the United States, other countries, and even private companies put a lot of effort into attribution and they've gotten a lot better at attribution than they were ten or fifteen years ago. The question is: How good are we in attribution exactly?

> "If you are going to punish somebody for doing something in cyberspace that crosses your line, you have to have some notion of who they are. You need attribution.

To answer this question, you have to ask another question which is: What do you need attribution for? There are three reasons for it, but let us start with the first two. The first one is fairly obvious. You want to know that the guys you are punishing are the guys who did it. The second reason why you need high confidence in attribution is to be able to convince other people that in fact you've done this right. We live in a world in which if you create risks by retaliating, you need a way of justifying them. This creates a dilemma, because you may be certain in your own mind, using your resources and methods, that you have put your finger on the right person. But if you cannot convince the rest of the world about it, then you are going to have a problem justifying either causing harm to this other party or creating the risks that come when you hit somebody who clearly can fight back because that was what started the entire confrontation in the first place. How good does this attribution need to be? It's not a court room, so you don't need to prove attribution beyond the shadow of a doubt. However, you do have to strike a strategic balance. On the one hand, if you are unsure about attribution and you don't punish anybody, this will create a precedent in cyberspace that misdeeds go unpunished. If you do, however, punish someone and it turns out to be the wrong person – that is a risk, too. And therefore, you have to balance the risk. Am I better off making a mistake and punishing someone, or am I better off not making a mistake and not punishing anybody? There's a constant trade-off involved here.

For the U.S. and any other country, there's another trade-off that has to be made. What do I reveal about how I came to the conclusion that this particular party did it? In 1962, during the Cuban Missile Crisis, Dean Acheson went to Charles De Gaulle. He said: 'Mr. President, we need your support and I've got pictures in my briefcase that will prove to you that the Soviet Union has nuclear weapons in Cuba.' And Charles de Gaulle said essentially: 'The word of the American president is enough. If he says that there are missiles in Cuba, I don't need to see the photographs.' It is not going to come as a surprise that we do not live in that world anymore. Nowadays, neither the U.S. nor any other country frankly can say: 'Trust me, I know there was an attack by this party and you have to believe me.'

To date, we've made only modest attempts to try to demonstrate why we knew that a particular country had done it. For instance, in late 2014, the U.S. government wished to make the case that Sony was attacked by North Korea. So, the Department of Justice put out a press release. It had a lot of words in it, exactly 140 words of which made the case that North Korea had done it. Later it turned out that there was other evidence that was leaked to The New York Times which made a better case, but the U.S. said that they would enact countermeasures well before those leaks had become public. When it came to assigning fault to the hacks of the Democratic National Committee, the explanation was even worse. In fact, there were some technical errors that appeared in one of the explanations, which was produced by the DHS and the FBI. The justification that was part of the intelligence community's document was fairly close to a 'trust me' and then two-thirds of the document was about television company called RT. In neither part was it was particularly convincing.

So far, we have been living in a world in which the consequences of attacking another country in cyberspace have varied from relatively non-existent to fairly mild. A world in which there are no consequences of misbehaviour is a world in which you don't spend a lot of time trying to practice operational security. In other words, you don't take the time and trouble to be careful or avoid particular targets for fear that you

might be identified. If we, however, had a deterrence policy, there would be consequences for others carrying out a cyberattack. And if there were consequences for carrying out the attack, one could also reason that attackers would make more of an effort to hide their tracks. These days, we have a whole panoply of culprits that are fingered every time there's a cyberattack. There are companies like CrowdStrike, which has a fondness for animal names, FireEye, Symantec, to name but a few, which in fact have made identifying hacker groups part of their business in threat intelligence. It looks like we are pretty good at attribution. Unfortunately, we are pretty good at attribution in a world in which the consequences of attribution are relatively mild. If deterrence were to prevail, it would make attribution become difficult.

Let us talk about the word 'This'. When you have a deterrence policy, you have to communicate one way or another in advance what actions by the other side are going to merit punishment. You don't need an extremely high degree of precision – particularly one so detailed that the other side concentrates on looking for loopholes in your strictures. But you do have to convey a general sense of what not to do. What general sense would other countries have of the U.S. tolerance for a cyberattack? Well, it is well understood that the United States could not let pass a cyberattack with the consequences of the 9/11 hijackings, which left 3,000 dead and wreaked about 200 billion dollars' worth of damage. We know a lot of attacks have not garnered U.S. notice, so they are probably below the threshold. But where the thresholds lie in the vast space between 9/11 and a Sony-lite attack remains a question.

If we talk about military consequences, life and death happen to be binary and hence thresholds framed in such terms are straightforward to relate and measure against. The U.S. carried out a retaliation strike against Libya in 1986 for the death of two servicemen in a Berlin discotheque terrorist bombing. The U.S. went to war with Mexico in 1846, because of an incident in which 11 people died north of the Rio Grande river border. It doesn't take many casualties to actually justify a threshold. But that isn't a particularly useful guidance in cyberspace, because the next cyberattack that kills somebody will be the first cyberattack that kills somebody. You can end up with hundreds of millions of dollars in damage very easily with nobody even having a hair harmed on their head. It is a field in which the metrics of warfare that we're used to just don't apply very well.

> "When you have a deterrence policy, you have to communicate one way or another in advance what actions by the other side are going to merit punishment.

What would the U.S. or any other country establish as a threshold? One could say that an attack on critical infrastructure could be one of them. That has a notion of clarity, even though it doesn't really say to what extent an attack on an infrastructure could be considered actionable. There is also another question. What constitutes infrastructure? The U.S. objected to the North Korean attack on Sony in 2014. Was Sony Entertainment Corp. part of the national critical infrastructure? The few people who said 'yes' were laughed out of court. What about the attack on the Democratic National Committee? Was that a part of the critical infrastructure? Not really, although afterwards the U.S. defined the election machinery as a part of the critical infrastructure. If you are going to have a definition, it doesn't really do you good to make the definition clear after the fact. That doesn't give you the kind of deterrence you want.

Someone else in the Department of Defence basically said: 'We are not going to go after every cyberattack; we are just going to go after the 2% of all the cyberattacks.' The problem is there is no lower limit on a cyberattack. And those of you who majored at math know that 2% of an undefined set is itself an undefined set. Do you have transcendent values at stake? And if so, if you haven't declared them, what is the other side going to assume on your transcendental values or about the legitimacy of your transcendent values? Bear in mind that this is a world in which the U.S. talks about

cybersecurity and our rivals talk about information security – which covers a very different set of transgressions. This is a puzzle in itself.

So if you are going to have a threshold, you will probably want to measure it in terms of money. However, there are certain measurement problems that complicate how we know how much damage has taken place.

What about the nuclear era? Were we terribly precise about these things? As it was, nobody wanted to test the boundaries in the nuclear era because the consequences of getting them wrong were catastrophic. The consequences of facing retaliation in cyberspace don't look so grim, which means that you can expect a lot more testing. So you can't just say you find some actions unacceptable and expect the kind of deterrence that you want.

Let's now focus on 'I will', which is the business of credibility. You may make all sorts of threats, but how does the other side know you are going to carry them out? In truth, we haven't had a lot of retaliation in cyberspace. Nobody has. I think the U.S. has tried twice. Nobody else has publicly tried. Probably the only country that has credibility is Israel because they constantly do retaliation. But when it comes to the U.S., there have only been two cases in which the U.S. announced retaliatory actions. One of them was North Korea, and the other was Russia. What did we do to North Korea after saying that we would do something to them? If you have an answer to that question, you know more than I do. When President Obama announced retaliation, he said there would be some things we would see and some things we wouldn't see. Having seen nothing, I don't know what to say about the things that I haven't seen, and worse, nobody on the outside knows either. The U.S. had promised to retaliate against North Korea and but, as far as anybody knows, did nothing. The U.S. had promised to retaliate against Russia. Again, some reprisals were going to be visible and others not. So, what did we see? We saw the U.S. kicking a number of Russian diplomats out of the U.S. and we saw the U.S. close some Russian facilities in the United States. Was that impressive? This is the world of diplomacy and under the rules of diplomacy you can pretty much kick out any diplomat anytime you want for any reason whatsoever or for a no reason at all. Countries putting their diplomats in other countries understand that it's the nature of diplomacy. Later, Russia did that back to us when they realised that the new administration wasn't going to reverse the decision the old administration had made. Kicking out diplomats was a signal that the U.S. government disapproved of what Russia had done, but it didn't make Russia quake in its boots as a result.

> "You may make all sorts of threats, but how does the other side know you are going to carry them out? In truth, we haven't had a lot of retaliation in cyberspace.

Let's discuss the last thing, which is 'That'. 'That' is the belt here. What kind of punishment can the U.S. levy? Getting back to Admiral Rogers, he wants a bigger belt. But how big is the belt we already have? If you, as another country's leader, had to guess what the U.S. can do, you've got two benchmarks. One is Stuxnet, which the U.S. has never officially admitted to, but which everybody assumes that the U.S. did. The other comprises Snowden's revelations, none of which the U.S. has admitted to, but most of which everybody considers to be accurate descriptions of capabilities. We need to remember that deterrence is always in the mind of the other party. It's not in our mind. In that sense, the U.S. has a great deal of potential capability as shown by what it did in the past. Capability in cyberspace is not assessed in the same way as it is with other forms of force. In cyberspace, you cannot look at the piece of code and say: 'Oh, I know what this will do' because everything depends on the vulnerabilities and the dependence of the other side. A cyber weapon which may be good against Peru may not necessarily work against North Korea because the North Korea is called a 'Hermit Kingdom' for a reason. They're isolated from the rest of the world and they are not terribly well digitized either. I think somebody has actually counted the number of websites in North Korea and it turned out to be a staggering number of 23. That's not a country against which you can easily make a credible cyber threat.

In recent months, Tom Bossert, who is the assistant for Homeland Security for the current administration, basically said: 'People think that we are going to retaliate a cyberattack with something cyber of our own, but in fact the U.S. is going to use all instruments of power as a way of responding to a cyberattack.' As good as it sounds, it doesn't solve the problem – and having other options deprecates the value of having an offensive cyberspace capability.

So what would a possible hierarchy of punishments could look like? At the low end, you can start with talking or – as it's popularly known – 'naming and shaming'. However, naming and shaming doesn't work against shameless adversaries. I mentioned diplomatic manoeuvres, which are not particularly effective either. What about hauling the perpetrators to jail? The U.S. Department of Justice indicted five members of the Chinese People's Liberation Army and seven scientists from Iran. It's some kind of inhibition against their hacking, but not a particularly great one if they never expect to see the inside of a US courtroom.

> "We need to remember that deterrence is always in the mind of the other party. It's not in our mind.

Mr Bossert was also talking about the economic leverage. The U.S. has an unequalled economic leverage, in part because it houses a large percent of the world's financial infrastructure. Against many countries, it would be decisive, but the problem is you cannot boycott the same country twice for the same thing. You cannot threaten to not trade with North Korea if they carry out a cyberattack because we already don't trade with North Korea. You only have so much leverage. If you've used it for other things, that's that much less leverage you have for all the other insults and injuries that a country can do to you.

In cyber, we can raise the ante to kinetic. There was a quote that appeared in the Wall Street Journal about five years ago, which essentially said: 'If you take down our power grid, we are going to put a cruise missile down your smokestack.' This risk we call war. And if you think that a cyberattack is expensive, try totalling up the costs of a real 'honest-to-god' war. The U.S. went into Iraq and has spent, by various estimates, 1 to 3 trillion dollars, which is a lot of money. And the risk of war, the risk of responding to a nonviolent attack with violence has to be taken very seriously by those people weighing reprisal options. Conversely, you don't want other people to think you are never going to use military force, even if you are probably never going to use it.

So, those are the four things that we have to keep in mind: attribution, thresholds, credibility, and capability. But even then, your deterrence may not necessarily work. Your adversaries may believe that the benefits of an attack actually exceed the cost of it -- particularly, if it's an adversary or a regime that is not certain of its place in the world. Even though we think that the punishment may deter, there may be some cases where it is simply not enough.

The second issue is legitimacy. Are countries are being told not to do things which they think they are allowed to do. A lot of people will look at a cyberattack as a retaliatory act against something that happened earlier. North Korea argued, even if their arguments didn't resonate outside the country, that since their leader had been insulted, they were justified, and in fact attacking Sony was a response to the insult. But legitimacy is a broader issue. The U.S. knows that the Chinese have taken irritation at the anti-circumvention tools that they hosted on GitHub. But I think that the Chinese also know that they couldn't punish the U.S., or even talk that they were going to punish the U.S. for allowing GitHub to exist, because they don't think we believe that's a legitimate deterrent threat.

Thus while the four elements are necessary to have a deterrence policy, but they are not always sufficient.

In working through the deterrence challenge it may help to ask: why would you want a deterrence policy? The reason is to reduce the expectation of loss in comparison to a world in which you don't have a deterrence policy. Everything depends on how much you think you will lose as a result of cyberattacks if you do nothing.

That's a tricky question. There are people who say that if we don't have deterrence, someone is eventually going to take down the U.S. power grid or scramble the records of the U.S. banking system. If you look at the past, the losses to state actors from cyberattacks (cyber espionage is a totally different story) have not been terribly impressive compared to the costs that are commonly spent on national defence.

But does the past always predict the future? If you had asked somebody about the benefits of deterring physical terrorism in the year 2000, and looked at the pattern of foreign acts of terrorism in the United States, even the aggregate cost is not all that large. In 2001, there was a several order magnitude shift in our perception of what terrorists could do. If the world of the future looks like the world of the recent past, the need for a cyber deterrence policy is relatively low. But if we're in a period such as before 2001, where the past is really no good guidance the costs of the future, then you do need a deterrence policy in one shape or the other. And when you need a deterrence policy, let's hope that it's more than just 'I've got a really big belt'. ■

The article is a transcript of the presentation delivered on 10 October 2017 at the 3rd European Cybersecurity Forum – CYBERSEC 2017 in Krakow, Poland.

CYBERSEC

EUROPEAN
CYBERSECURITY FORUM

DON'T MISS THE 4TH EDITION

SAVE THE DATE 8–9 OCTOBER 2018

FOLLOW US ON:

#CSEU18

WWW.CYBERSECFORUM.EU

ANALYSIS

A BALANCE OF POWER IN CYBERSPACE

DR. ALEXANDER KLIMBURG
is Director of the Global Commission on the Stability of Cyberspace (GCSC) Initiative and Secretariat, and Director Cyber Policy and Resilience Program at the Hague Centre for Strategic Studies (HCSS). He is a non resident senior fellow with the Atlantic Council, a former associate and research fellow of the Harvard Kennedy School's Belfer Center, and an associate fellow at the Austrian Institute of European and Security Policy. His most recent book, "The Darkening Web: the War for Cyberspace" was published by Penguin Press.

Dr. Klimburg has worked on numerous topics within the wider field of international cybersecurity since 2007. He has acted as an adviser to a number of governments and international organizations on national cybersecurity strategies, international norms of behavior in cyberspace and cyber-conflict (including war, cyber-crime, and cyber-espionage), critical infrastructure protection, and Internet governance.

LOUK FAESEN
is Strategic Analyst at the Cyber Policy and Resilience Program of the Hague Centre for Strategic Studies. He mainly focuses on international cybersecurity, especially legal and political norms of responsible state and non-state behavior in cyberspace. He also functions as the Project Manager of the Global Commission on the Stability of Cyberspace (GCSC) Secretariat. Louk worked previously as a Policy Officer at the Task Force International Cyber Policy of the Ministry of Foreign Affairs of the Netherlands, where he assisted in the substantive preparations of the Global Conference on CyberSpace 2015 (GCCS) and the Global Forum on Cyber Expertise (GFCE) in The Hague, as well as subsequent projects related to international peace and security in cyberspace, such as the application of international law, confidence building mechanisms, and norms of responsible state behavior.

1. Introduction

Cyberspace[1] is managed by stakeholders from civil society, the private sector, and, to a lesser degree, by governments. The latter, however, is increasingly asserting its role in cyberspace, leading to a redistribution of power in which States are not only competing with other stakeholders, but also amongst each other. All cyberspace users thus face a power struggle between States that stands to affect the private sector and civil society, the multi-stakeholder approach to managing Internet resources, and therefore cyberspace writ large.

This article appropriates a realist model in international relations – the balance of power theory (BOP) – and adjusts it with neoliberal concepts of power to help better understand the challenge of stability between States in and on cyberspace. It specifically enables the "cybered" international relations of governments to be analysed against the backdrop of the complex ecosystem of stakeholders. This does not presuppose that States are or should be the most important or influential actors in cyberspace. Instead, this article focuses on State interests. It identifies two conditions of the BOP theory and applies them to cyberspace in three different scenarios previously suggested by States, and offers one suggestion on the way forward.

2. The Balance of Power

"The greatest need of the contemporary international system is an agreed concept of order. In its absence, the awesome available power is unrestrained by any consensus as to legitimacy... without it stability will prove elusive".[2]

The balance of power theory is one of the most enduring and protean concepts in international relations.[3] It has also sometimes proven to be the battle line between both neorealist and neoliberal interpretations in international relations scholarship. This largely has been because of different interpretations of the term "anarchy" in international relations, and different assessments of the propensity of States to actually collaborate, besides a fundamentally different assessment of what constitutes "power". This has sometimes amounted to wasted opportunity, since it is possible to apply more neoliberal views to BOP, both by stressing the importance of institutions as well as including a wider concept of power per se. This is even possible when taking many neorealist positions as a starting point.

For instance, a common point of departure for BOP is the basic assumption that States act rationally to maximise their security or power in anarchic systems without a higher authority to regulate disputes.[4] Robert Jervis lists four realist assumptions that constitute the foundation of this premise: (i) all states must want to survive, (ii) they are able to form alliances with each other based on short-term interests, (iii) war is a legitimate instrument of statecraft, and (iv) several of the actors have relatively equal military capabilities.[5] The system ensures that any one State's power will be checked by a countervailing (coalition of) power that is alarmed by the potential hegemonic threat it poses to the system. From here on forward, the perspectives on the BOP theory diverge: one of them views the active goal of States as pursuing strategies designed to maintain the balance, while another maintains that it is an automatic consequence

[1] US National Security Presidential Directive 54/Homeland Security Presidential Directive 23 (NSPD-54/HSPD-23) defines cyberspace as "the interdependent network of information technology infrastructures, and includes the Internet, telecommunications networks, computer systems, and embedded processors and controllers in critical industries. Common usage of the term also refers to the virtual environment of information and interactions between people."

[2] Henry Kissinger, "Central Issues of American Foreign Policy", 1969, available at: https://history.state.gov/historicaldocuments/frus1969-76v01/d4

[3] For an overview of the evolution of the balance of power theory, see Rendall L. Schweller, "The Balance of Power in World Politics", May 2016, Oxford University Press, USA. For examples of the competing theoretical and empirical claims see J. A. Vasquez and C. Elman (Eds.), "Realism and the balancing of power: A new debate." Saddle River, NJ: Prentice Hall.

[4] See for example Mearsheimer: "The international system creates powerful incentives for States to look for opportunities to gain power at the expense of rivals, and to take advantage of those situations when the benefits outweigh the costs" (John Mearsheimer, "The tragedy of great power politics", 2001, New York: Norton); and Morgenthau: "the aspiration for power on the part of several nations, each trying to maintain or overthrow the status quo, leads of necessity, to a configuration that is called the balance of power and to policies that aim at preserving it", (Hans Morgenthau, "Politics among nations: The struggle for power and peace" (4th ed.), New York: Alfred Knopf).

[5] Robert Jervis, "Cooperation under the Security Dilemma",1978, pp.186-189.

of State behaviour, a side-effect.[6] As its name implies, the distribution of power, usually defined in terms of military capabilities, is central to the BOP theory.[7] In particular, rough parity among several competing actors is frequently posed as a necessary feature of such a system. Even though the invisible hand of the balance of power regulates the system, States must be moved by explicit concerns over a potential hegemon and be ready to counter it with checks and balances as they struggle to curb the rise of a potential hegemon. As we shall see later, this becomes complicated if one departs from the realist definition of power as being purely military and adopts a wider understanding of what power may entail.

Fundamentally, the balance of power is based on a compromise – it cannot satisfy every actor in the international system completely. It works best when it keeps one State from predominating and prescribing laws to the rest, and prevent the aggrieved parties from seeking to overthrow the international order. It does not purport to avoid crises or even wars. Its goal is not aimed at reaching peace, but rather moderation and stability.

"Paradoxically, the generality of dissatisfaction is a condition of stability, because were any one power totally satisfied, all others would have to be totally dissatisfied. The foundation of a stable order is the relative security – and the relative insecurity – of its members." [8]

[6] Waltz, for instance maintains that "these balances tend to form whether some or all States consciously aim to establish and maintain balance, or whether some or all States aim for universal domination" in Waltz K.N., "Theory of International politics", 1979, Reading, MA: Addison-Wesley, p.119; and Morgenthau who considers a balance of power as a result from a State's policies in Hans Morgenthau, "Politics among nations: The struggle for power and peace" (4th ed.), New York: Alfred Knopf. Statecraft based on balancing polices has been lauded by figures such as Metternich, Castlereagh, Churchill, and Kissinger.

[7] Schweller, R. L., "Unanswered threats: Political constraints on the balance of power", 2006, Princeton, NJ: Princeton University Press: "Balancing means the creation or aggregation of military power through either internal mobilization or the forging of alliances to prevent or deter the occupation and domination of the State by a foreign power or coalition. The State balances to prevent the loss of territory, either one's homeland or vital interests abroad (e.g., sea lanes, colonies, or other territory considered of vital strategic interest). Balancing only exists when States target their military hardware at each other in preparation for a possible war."

[8] Henry Kissinger, "A World Restored: Metternich, Castlereagh, and the Problems of Peace 1812-1822", 1957.

2.1 Defining Cyber Power

Traditional understanding of the balance of power where States seek to survive as independent entities in an anarchic global system can seem particularly challenged when confronted with the concepts of *cyber power*. In a contemporary world with powerful norms against conquest, States no longer fear the same degree of physical extinction. The empirical evidence of limited military intervention for balancing purposes attests to the need to expand the traditionally military-security notion to include a wider range of means – including not only economic but also "soft power" factors.[9] Indeed, the challenge is that in cyberspace many (but not all) of the traditional realist measures of State power do not seem to hold up, and it is therefore necessary to reconceive of what power means in cyberspace.

Power, however elusive and difficult to measure, goes beyond the physical or military supremacy over another. Joseph S. Nye offers guidance by describing *cyber power* as a unique hybrid regime of physical properties (the infrastructures, resources, rules of sovereignty and jurisdiction) and virtual properties that make government control over the former difficult. Low-cost attacks from the virtual or informational realm can impose high impacts and costs on the physical layer. The opposite is also true; control over the physical layer can have territorial and extraterritorial effects on the virtual layer.[10] Daniel Kuehl defines *cyber power* as "the ability to use cyberspace to create advantages and influence events in other operational environments and across the instruments of power."[11] In line with his distinction between hard and soft power, Nye conceptualises three faces of power: (i) the *coercive* ability to make an actor do something contrary to their preferences or strategies, (ii) *agenda setting* or framing to preclude the choices of another by exclusion of their strategies, and (iii) *shaping* another's initial preferences so that some strategies are not even

[9] See Joseph S. Nye, Jr., "The Future of Power", 2011 *Public Affairs*.

[10] Joseph S. Nye, Jr., "Cyber Power", 2010, Harvard University Belfer Center for Science and International Affairs, pp.7-8. Available at: www.belfercenter.org/sites/default/files/legacy/files/cyber-power.pdf.

[11] Daniel T. Kuehl, "From Cyberspace to Cyberpower: Defining the Problem," in: Franklin D. Kramer, Stuart Starr, and Larry K. Wentz, (eds.), "Cyberpower and National Security", 2009, Washington, D.C.: National Defense UP. Available at: http://ctnsp.dodlive.mil/files/2014/03/Cyberpower-I-Chap-02.pdf.

considered.[12] This article focuses on the first face, gives a cursory glance at the second, and only touches upon the third. This is not a reflection of relative importance of the respective faces of power (indeed some scholarship might consider the opposite to be the case), but rather a focus on the measurability (or at least observability) of the faces of power: the third face is difficult to capture using traditional international relations methods.

The *hard power* manifestation of the first face of power in cyberspace, which comes close to the realist interpretation of power, is the ability to infringe on the availability and integrity of data. This can be accomplished either through denial of services (e.g. DDoS) or by various methods designed to influence data integrity (e.g. destructive malware insertion by various means). To accomplish these activities, some capability is often equally required in the non-kinetic field of "espionage" – i.e. the ability to violate the confidentiality of data. This precursor, formally known as Computer Network Exploitation (CNE)[13], has since been refined to include capabilities known as ISR (intelligence, surveillance and reconnaissance) and OPE (operational preparation of the environment, a.k.a. "preparing the battlefield").[14] Thus, it is logical that the capability of States to inflict kinetic-effect harm in cyberspace requires (to various extents) the ability to conduct intelligence gathering.[15] However, the exact nature of these "kinetic-equivalent" effects, formally simply known as "Computer Network Attack" and now known as "Offensive Cyber Effect Operations" (OCEO)[16], is in doubt. While some cyber capabilities are reserved for the battlefield (e.g. to take out a radar to enable an air strike) and are at least somewhat defined and even considered as "cyber fires,"[17] other capabilities are less clear. For instance, OCEO targeted at a power grid could of course mean "switching off the grid". But it could also mean "destroying the grid" to many different degrees, including to the extent that it was not easily reconstitutable. And finally, it could also mean something completely different – where for instance the power grid is simply repositioned to be used as an espionage tool[18], or even as a weapon itself. This lack of clarity on what exact capabilities in cyberspace are, means that it is very difficult to describe comprehensively what the "means" (delivery systems or weapons) are. In some cases, this might seem relatively easy – Stuxnet, Flame, Duqu Shamoon, Ouroboros, and Dark Energy, come to mind as examples of somewhat classifiable "cyber weapons", but in other cases this would be much more difficult. For the purposes of arms control or similar, the lack of transparency in presumed force deployment and even the method of operation or intended effects make the task extremely difficult, at least if an "arms control treaty" is the goal. At best, a "cyber weapon" remains a weapon system of "omni-use" technologies that is extremely difficult for another State to verify due to a lack of transparency. Otherwise, however, States are only left with the ability to presume – basically to guess – the overall capability of another State (albeit at widely variating degrees of detail) without, in most cases, being able to detail the exact order of battle, table of equipment, tactics, techniques and procedures or other basic information – unless the intelligence assessment is very complete.

Leaving the definitional hurdles aside, the equilibrium of forces or the military balance of power in cyberspace is further complicated by characteristics unique to these tools:

- The success of an attack is more a reflection of the overall quality of defence rather than the quality of offense. An attacker will therefore always use the "cheapest" tools available, and not necessarily the most advanced.[19]

[12] Ibid. p.10.

[13] CNE was initially defined in JP1-02 as "Enabling operations and intelligence collection capabilities conducted through the use of computer networks to gather data from target or adversary information systems or networks." In JP 3-13 (2012) its removal from JP-02 was approved.

[14] Cyberspace Operational Preparation of the Environment (OPE) is defined in JP3-12 (2013) as "consist[ing] of the non-intelligence enabling activities conducted to plan and prepare for potential follow-on military operations. OPE requires cyberspace forces trained to a standard that prevents compromise of related IC operations. OPE in cyberspace is conducted pursuant to military authorities and must be coordinated and deconflicted with other USG departments and agencies."

[15] Network attacks are usually preceded by network exploitation. As former NSA and CIA director Michael Hayden states in his book, "Playing to the Edge" (2017): "Reconnaissance should come first in the cyber-domain. … How else would you know what to hit, how, when — without collateral damage?"

[16] Offensive Cyber Effects Operations (OCEO) is defined in PPD-20 as "Operations and related programs or activities - other than network defense, cyber collection, or DCEO - conducted by or on behalf of the United States Government, in or through cyberspace, that are intended to enable or produce cyber effects outside United States Government networks."

[17] See FM3-38 (2014) for examples. Electronic Attacks, for example, is "considered a form of fires" (see 4-3).

[18] Exploiting, for instance, the ability to conduct differential power analysis on individual computers.

[19] Alexander Klimburg "The Darkening Web: the War for Cyberspace", 2017, Penguin Press.

- The vast majority of offensive cyber effects can only be deployed using civilian intermediaries (networks, products) that also can be part of a neutral or even friendly third nation.
- The difference between imminent preparation for attack (e.g. OPE) and simple espionage can be hard to distinguish for the defender, making inadvertent escalation much more likely due to a failure to correctly interpret intent.
- Offensive capabilities are much cheaper and much easier to develop and deploy than the total sum of necessary defensive measures.[20]
- Unlike conventional weapons, "cyber weapons" can be re-used but are also perishable – an entire arsenal can be rendered useless without ever being used once the vulnerability is patched.[21]
- These tools are specific – the outcomes are dependent on the victim's network – and can be immediate or time-delayed. They upend conventional ways of response.
- They can also be reverse engineered, weaponised and re-used by the victim or another party that gets their hands on the technology.[22]
- They do not only undermine the target's security, but also compromise the security of other actors using systems with the same vulnerabilities.[23]

[20] Rebecca Slayton, "What is the Cyber Offense-Defense Balance? Conceptions, Causes, and Assessment.", 2016, International Security 41, no. 3. Slayton argues that this perception leads to unnecessary escalation and militarization of cyberspace. According to Klimburg (2017), using DDoS costs as a point of departure, defense can be conceived as being up to 1,000 times more costly than offense.

[21] In "Zero Days, Thousands of Nights" by Lillian Ablon and Timothy Bogart of RAND, the average lifespan of zero-days is set at 6.9 years, and 'for a given stockpile of zero days, about 5.7 percent will be publicly disclosed after one year. The report is available at: www.rand.org/pubs/research_reports/RR1751.html.

[22] The EternalBlue exploit is a good example of a weapon or exploit developed by the NSA that was leaked by the Shadow Brokers, and was used in several malware epidemics afterwards, including NotPetya and WannaCry. See for example Thomas Fox-Brewster, "An NSA Cyber Weapon Might Be Behind A Massive Global Ransomware Outbreak", Forbes, May 12, 2017, www.forbes.com/sites/thomasbrewster/2017/05/12/nsa-exploit-used-by-wannacry-ransomware-in-global-explosion/#2ff505c2e599; and Nicole Perlroth, Mark Scott, Sheera Frenkel, "Cyberattack Hits Ukraine Then Spreads Internationally", The New York Times, June 27, 2017, www.nytimes.com/2017/06/27/technology/ransomware-hackers.html?_r=0.

These is just a small range of examples describing how the fundamental differences between cyber and conventional weapons greatly complicate the process of parsing State offensive cyber capabilities.

But even in the physical world, Kissinger states that "an exact balance is impossible, and not only because of the difficulty of predicting the aggressor. It is chimerical, above all, because while powers may appear to outsiders as factors in a security arrangement, they appear domestically as expressions of a historical existence. No power will submit to a settlement, however well-balanced and however secure, which seems totally to deny its vision of itself."[24] Power is thus conceived and assessed not merely as a mathematical exercise (the number of weapons or military capabilities), but takes into account the perception of a nation's leaders, the quality of its strategies, military doctrines, and its will to use power effectively. Therefore, the common perception of a State's cyber capabilities, even if founded on incomplete knowledge, can function as a basis for calculating the respective balance of power.

2.2 Legitimacy

According to Kissinger's theory, a balance of power is not in itself an adequate basis for order. It is regarded as a minimal condition, but if it becomes an end in and of itself, it becomes self-destructive: "a system based purely upon power will turn every decision into a contest of strength, whereas the essence of stability is the recognition of limits by major actors."[25]

If nations desire peace, they cannot seek it directly. Instead, they must focus on creating stable relations among nations, which, according to Kissinger, is based on two major conditions: the existence of a balance of power and the acceptance of an international system of mediation and legitimacy by the major powers – an acceptance he terms "the legitimizing principle" or "the principle of legitimacy".

[23] Several examples include NotPetya, Turla and Black Energy. These are all malware attacks generally thought to be sponsored by the Russian Federation. Nevertheless, it went rogue and the malware hit Russian organisations and companies as well. More information available at: www.cfr.org/interactive/cyber-operations

[24] Henry Kissinger, "A World Restored: Metternich, Castlereagh, and the Problems of Peace 1812-1822", 1957.

[25] Ibid. p.145.

These two terms should be conceptualised as conditions that form the basic hypotheses about the ideal conditions for the effective functioning of the system.[26]

"A balance of power makes the overthrow of international order physically difficult, deterring a challenge before it occurs. A broadly based principle of legitimacy produces reluctance to assault the international order. A stable peace testifies to a combination of physical and moral restraints." [27]

This brings us to the second condition of stability – which commonly results not from a quest for peace, but from a generally accepted legitimacy. It means no more than an international agreement about the nature of workable arrangements and about the permissible aims and methods of foreign policy. It implies the acceptance of the framework of the international order by all major powers, at least to the extent that no State is so dissatisfied that it expresses its discontent in terms of a revolutionary foreign policy. The legitimizing principle reflects the prevailing values of the historical epoch, especially how the international order should be organised in a specific context, and captures a general acknowledgement or consensus among the major actors in a system on what is considered to be the principal form of organisation and order (see more about the legitimizing principle in the side note)[28]. This principle identifies the what – the central actors – and the how – the types of interactions – in the international system. The peace of Westphalia, for example, marked a change in the legitimizing principle from feudalism to the system of sovereign Nation-States. The legitimizing principle is often summarized as a "recognition of limits" by the State. It is important to understand that these limitations are not necessarily only legal or institutional, but also include the understanding of what the actual and normative reality means.

In the context of cyberspace, the system for governing global cyber activities is primarily construed within its technical reality. The various interlocking but separate governance processes that together define cyberspace have been described by Joseph S. Nye as forming a "regime complex":[29]

This regime complex is only partially influenced by State actors, and by bilateral, regional, or multilateral processes. The private sector and civil society both generate products, common practices, and norms of behaviour largely separate from government involvement, although these developments can have significant impacts on State-led processes and discussions on international peace and security. Despite States' traditional dominance over all

[26] Randall L. Schweller, "The Balance of Power in World Politics", 2016.

[27] Henry Kissinger, "War Roared Into Vacuum Formed by a Sidestepping of Statesmanship", 1989, available at: http://articles.latimes.com/1989-08-27/opinion/op-1559_1_eastern-europe.

[28] The *legitimizing principle* is not a traditional element of the Balance of Power theory. Although the concept appears in other contexts and modes of thought, Henry Kissinger introduced it as an addition to Balance of Power in order to establish stability – see: Henry Kissinger, *A World Restored: Metternich, Castlereagh, and the Problems of Peace.* Similar definitions of the notion are included below:
"The legitimizing principle represents the prevailing values of the historical epoch. It is in the name of the legitimizing principle that nations accept the international order." In Gregory D. Cleva, Henry Kissinger and the American Approach to Foreign Policy, p. 66.

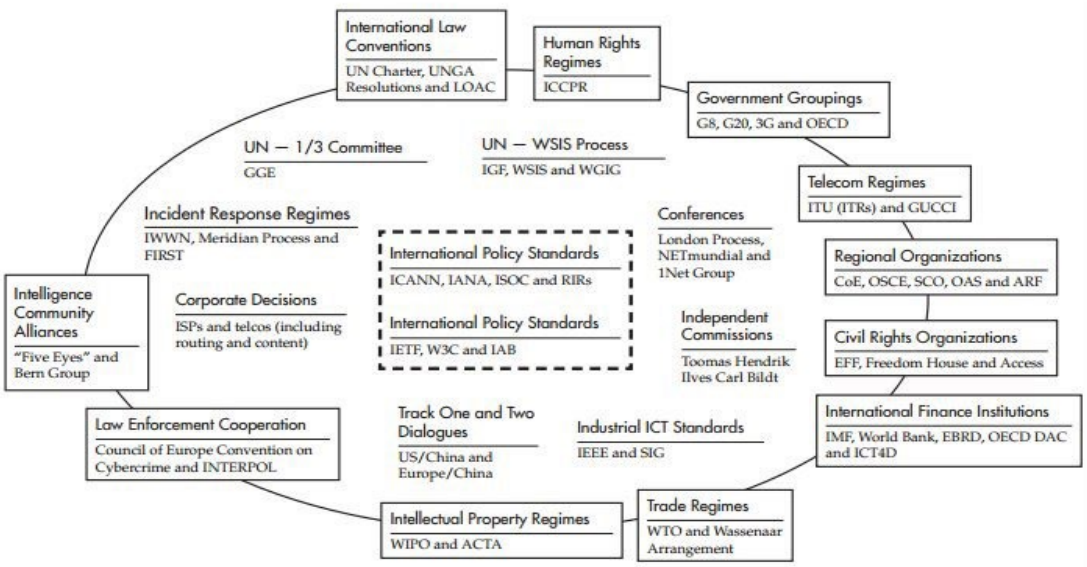
"By "order" is meant the legitimizing principle by which authority receives its sanction in the eyes of the association. […] It goes to the problem of discovering the operative ideals, the expectations, the rules of concerted action to which the group members believe it necessary to conform in order to give their leaders the necessary authority to realize their own desires and objectives."
In Avery Leiserson (1949), 'Problems of Representation in the Government of Private Groups.' The Journal of Politics 11, no 3: 569.

"The urge for formally declared and generally acknowledged legitimacy approaches the status of a constant feature of political life. This urge requires that power be converted into authority […]. Politics is not merely a struggle for power but also a contest over legitimacy, a competition in which the conferment or denial, the confirmation or revocation, of legitimacy is an important stake. […] [t]here is, of course, a correlation between the nature of the legitimizing principle and the identity of its applicator. For instance, the principle of divine right tends to call for an ecclesiastical spokesman, and the consent theory implies reliance on a democratic electoral process." In Inis L. Claude Jr. (1966), 'Collective Legitimization as a Political Function of the United Nations.' International Organization 20, no 3: 367.

"Legitimizing principles are called into question during major systemic crises, such as world wars or widespread political upheavals […]. This dynamic occurs because it is impossible to completely satisfy the statist and nationalist principles simultaneously. Therefore, the new system tends to generate its own crisis, leading to a reevaluation of the normative principle." In SJ Barkin and B Cronin (1994), 'The State and the Nation: Changing Norms and the Rules of Sovereignty in International Relations,' International Organization 48, no 1: 108.

[29] Joseph S. Nye, Jr. "The Regime Complex for Managing Global Cyber Activities", Global Commission on the Internet Governance, May 2014. Available at: www.cigionline.org/sites/default/files/gcig_paper_no1.pdf.

Figure 1. "The Regime Complex for Managing Global Cyber Activities". Source: Joseph S. Nye, 2014.[30]



questions related to international peace and security, governments make up only one out of three actor groups in the overall cyber regime complex, and its role within it is no greater than that of the private sector or civil society. The State-oriented regimes do not necessarily have the ability to speak on behalf of other equally crucial regimes. This creates a situation unique in international peace and security, where governments cannot decide on all aspects of the international cybersecurity domain itself, as responsibility and ownership for this domain is shared with non-State actors.

This could arguably be described as the multi-stakeholder reality of the domain. While the term does not have a single overriding definition, it does have an implicit definition. Its core idea is that some issues are too complex and have too many independent operational stakeholders to be decided on by one inevitably self-interested group and therefore require the participation of all stakeholders: civil society (including academia and technical community), the private sector, and governments. For the Internet, this is seemingly grounded in reality. It is the members of civil society (which includes State-funded university researchers, as well as corporate engineers working on their own time) who write the code of the Internet. It is the private sector that builds and owns most aspects of the Internet, ranging from the cables to the services, to products and software which runs on and in it. Government's role is relatively limited in that respect. Its power is manifested through its sovereign rights and jurisdiction.

Given this complex landscape, it is unlikely there can be a singularly encompassing entity successfully acting unilaterally across the entire regime complex. If, for instance, governments, as an overall actor group, were to agree to make definitive changes to the current non-State dominated Internet governance structures, then there would almost certainly be a strong reaction – not only from the private sector, but also from the engineers and hobbyists who have coded most of the backbone of the Internet. Installing an intergovernmental organisation instead of, for instance, the Internet Engineering Task Force, would not simply make these volunteers stop working on Internet technology. Therefore, the most basic reality of the wider cyber regime complex is that it is in its own, precarious, multi-stakeholder balance. While States can and may expand their own arrangements amongst each other, certain basic realities of how the domain is managed cannot be changed. Nothing that completely goes against the diffused power structure of cyberspace can therefore be considered viable or "legitimate" – the multi-stakeholder approach is therefore, in effect, the Westphalian System of the Internet.

[30] Ibid.

3. Balancing Power in Cyberspace

Thus far, it has become apparent that an equilibrium of State forces in cyberspace remains elusive because of the lack of a basic understanding of each other's capabilities and doctrines and therefore also a minimum amount of agreed definitions. Moving beyond power, the legitimizing principle reflects the recognition of the limits of States in the prevailing reality of the historical epoch. In cyberspace, this arguably can be expressed as the multi-stakeholder approach because of the technical reality of cyberspace that prevents one party from deciding universally and unilaterally.

From a State perspective, there are different ways to achieve a balance of power. In the next section, the guiding principles will be applied to three scenarios proposed by States that roughly correspond to the first three Committees of the UN General Assembly to see how likely they can actually lead to a balance of power that upholds to the legitimizing principle. This does not mean that the UN is or should be the sole means through which to establish international peace and stability in cyberspace. Instead, it offers a starting point to identify initiatives that have been previously proposed by governments, and one suggestion on the way forward.

3.1 First Basket, First Committee Issues

The First Committee of the United Nations General Assembly deals with issues of disarmament and international security. As previously mentioned, States make up only one of the three actor groups within the overall cyber regime complex despite their traditional dominance over all questions related to international peace and security in cyberspace, meaning they cannot decide on all aspects by itself – ownership is shared with the private sector and civil society. Yet, the involvement of non-State stakeholders in the international State-led processes remains limited at best. The last UN GGE Consensus Report (described below) seems to acknowledge the need to involve other stakeholders in its conclusions: "while States have a primary responsibility to maintain a secure and peaceful ICT environment, effective international cooperation would benefit from identifying mechanisms for the participation, as appropriate, of the private sector, academia and civil society organizations."[31]

[31] UNGGE 2015 Report, paragraph 31 on p.13, available at www.un.org/ga/search/view_doc.asp?symbol=A/70/174.

Using Nye's cyber regime complex as a point of departure, one of the authors expands Joseph Nye's regime complex to offer an impression of the stakeholders and respective processes affecting the political-military dimension of cybersecurity, a.k.a. "international cybersecurity" or "international peace and security in cyberspace" that could be considered UN First Committee issues.

In the UN context, the First Committee is most concerned with guiding responsible State behaviour in terms of international peace and security in cyberspace. To this end, here have been three major Sate efforts in the UN:[32]

1) The United Nations Group of Governmental Experts on Developments in the Field of Information and Communications Technologies in the Context of International Security (GGE).

Since its inception in 2010, the GGE has convened five times and issued three consensus reports. Each group had a mandate of only one year – which, until now, has been renewed on an annual basis. The first consensus report recommended that States consider norms, confidence building measures, and capacity building initiatives to "reduce the risk of misperception" in cyberspace.[33] In the second consensus report, major powers explicitly recognised for the first time the application of "international law, in particular the Charter of the United Nations, is essential to maintaining peace and stability in cyberspace.[34] It also encouraged the development regional Confidence Building Measures. The third consensus report outlines voluntary peacetime norms States are encouraged to follow. The 2016-17 iteration failed to reach a consensus report. The stumbling block: the application of international law to cyber operations.[35]

[32] For a comprehensive overview of cyber diplomatic initiatives see: Alex Grigsby (2017), "Overview of Cyber Diplomatic Initiatives", and Deborah Housen-Couriel (2017), "An Analytical Review and Comparison of Operative Measures Included in Cyber Diplomatic Initiatives", both published as Briefings from the Research Advisory Group for the Global Commission on the Stability of Cyberspace, available at: https://cyberstability.org/wp-content/uploads/2017/12/GCSC-Briefings-from-the-Research-Advisory-Group_New-Delhi-2017.pdf.

[33] The UN General Assembly, Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security, A/65/201 (July 30, 2010), available at: www.unidir.org/files/medias/pdfs/final-report-eng-0-189.pdf.

[34] The UN General Assembly, Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security, A/68/98 (June 24, 2013), www.un.org/ga/search/view_doc.asp?symbol=A/68/98.

[35] The United States argues it failed over states' unwillingness to explain how specific bodies of international law, such as the law of armed conflict

2) Members of the SCO have circulated a draft international code of conduct for information security at the UN General Assembly.[36]
The code proposes that countries voluntarily forego the "use of [ICTs] … to carry out activities which run counter to the task of maintaining international peace and security." It predominantly focuses on interstate cooperation against the use of ICTs to incite the "three evil –isms": terrorism, separatism or extremism, as well as reinforce the notion of non-interference in the internal affairs of States through ICTs. The code has been floated at the UN since 2011 but has attracted criticism for its perceived incompatibility with human rights law.[37]

3) Finally, the UN General Assembly adopted a resolution in 2003, calling on states to build a culture of cybersecurity by encouraging domestic stakeholders to be aware of cybersecurity risks and to take steps to mitigate them.[38]

Other multilateral initiatives to enhance international security and stability have been agreed outside of the auspices of the UN, most notably, the work of the Organization for Security and Cooperation in Europe (OSCE), the ASEAN Regional Forum (ARF), and other regional organisations on Confidence-Building Measures (CBMs). In addition, previous efforts have been made towards potential control of "intrusion software" by the Wassenaar Arrangement that aimed at "creating consensus approach to regulate conventional arms and dual-use goods and services."[39] It has 41 signatories that regulate the export of both conventional weapons and dual-use goods, which includes certain categories of information systems.[40] In 2013, the Member States agreed to include certain categories of intrusion software to this list.[41] Although this may bolster States against network intrusions, it also significantly impedes the ability of information security researchers to exchange findings without risking criminal proceedings.

Despite these efforts, 2017 marked the shortcomings of meaningful interstate efforts to advance norms and legal interpretations to bring international security and stability. This is just one way to do so. Some experts foresee a more fruitful future for operational cooperation – e.g. in CBMs[42], while others are exploring countering efforts to the proliferation of offensive cyber capabilities.[43]

(LOAC) or state responsibility, apply to cyberspace. Cuba, echoing the views of Russia and China, argues that acknowledging LOAC would legitimize cyberspace as a domain for military conflict, giving state-sponsored cyber operations a green light. Sources: Michele G. Markoff, "Explanation of Position at the Conclusion of the 2016-2017 UN Group of Governmental Experts (GGE) on Developments in the Field of Information and Telecommunications in the Context of International Security," available at: www.state.gov/s/cyberissues/releasesandremarks/272175.htm. "71 UNGA: Cuba at the final session of Group of Governmental Experts on developments in the field of information and telecommunications in the context of international security," Cuba's Representative Office Abroad, available at: http://misiones.minrex.gob.cu/en/un/statements/71-unga-cuba-final-session-group-governmental-experts-developments-field-information. For a non-State expert commentary of the failure of the 2016-2017 GGE, see for example: James A. Lewis, "The Devil Was in the Details: The Failure of UN efforts in Cyberspace", August 6, 2017, available at: www.thecipherbrief.com/devil-was-details-failure-un-efforts-cyberspace-1092.

[36] The UN General Assembly, Letter dated 9 January 2015 from the Permanent Representatives of China, Kazakhstan, Kyrgyzstan, the Russian Federation, Tajikistan and Uzbekistan to the United Nations addressed to the Secretary-General, (A/69/723) January 13, 2015, available at: https://ccdcoe.org/sites/default/files/documents/UN-150113-CodeOfConduct.pdf.

[37] The UN General Assembly, Letter dated 12 September 2011 from the Permanent Representatives of China, the Russian Federation, Tajikistan and Uzbekistan to the United Nations Addressed to the Secretary General, A/66/359 (September 14, 2011), available at: www.un.org/ga/search/view_doc.asp?symbol=A%2F66%2F359&Submit=Search&Lang=E ; Alex Grigsby, "Will China and Russia's Updated Code of Conduct Get More Traction in a Post-Snowden Era?" Net Politics (blog), the Council on Foreign Relations, January 28, 2015, available at: www.cfr.org/blog/will-china-and-russias-updated-code-conduct-get-more-traction-post-snowden-era; Sarah McKune, "An Analysis of the International Code for Conduct for Information Security," the Citizen Lab, September 28, 2015, available at: https://citizenlab.ca/2015/09/international-code-of-conduct/.

[38] The UN General Assembly, Resolution 57/239, Creation of a global culture of cybersecurity, A/RES/47/239 (January 31, 2013), available at: www.oecd.org/sti/ieconomy/UN-security-resolution.pdf.

[39] The Wassenaar Arrangement was criticized as lacking in technical expertise – partially because governments had no prior history of engaging with issues related to cyber security. For similar point see: Goodwin and Fletcher, "Export Controls and Cybersecurity Tools".

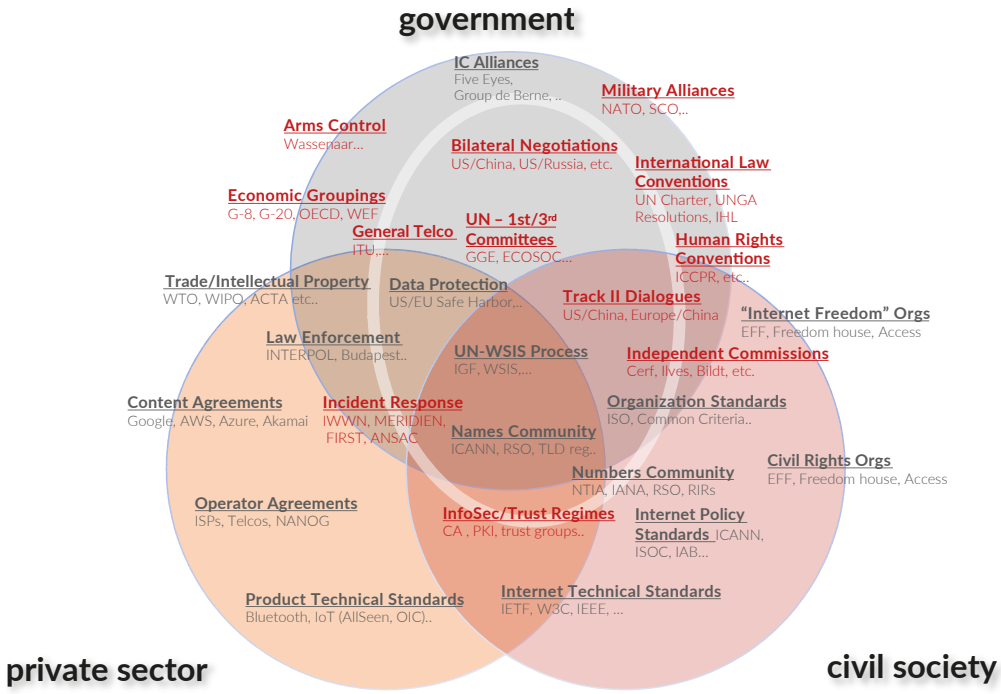
[40] More information available at: www.wassenaar.org/about-us/

[41] More information available at: www.wassenaar.org/wp-content/uploads/2015/06/WA-Plenary-Public-Statement-2013.pdf

[42] Alex Grigsby, "The End of Cyber Norms", Survival, 59(6), 2017.

[43] Robert Morgus, Max Smeets, Trey Herr, "Countering the Proliferation of Offensive Cyber Capabilities", 2017, published by the Global Commission on the Stability of Cyberspace, and available at: https://cyberstability.org/wp-content/uploads/2017/12/GCSC-Briefings-from-the-Research-Advisory-Group_New-Delhi-2017.pdf.

Figure 2. The Cyber Regime Complex by Stakeholder Group: the "International Cybersecurity" cluster is marked in red. Source: Alexander Klimburg, 2016.[44]



The most promising but also most difficult application of a balance of power framework would be through the traditional area of arms control. As noted before, the notion of what constitutes a "cyberweapon" is as open and contentious as the concept behind "cyber power" per se, and there is no definition of a cyberweapon or even cyber capabilities that would lend itself to negotiations. Russia/China and the United States still view cyber threats in fundamentally different ways (e.g. cyber tools versus information weapons), making it difficult to establish and enforce such a framework. There are some workarounds that have been suggested, such as the focus on simply regulating certain "effects" rather than trying to define the weapons. However, they also stumble over some basic differences in understanding of international law.

Currently, the open questions in international law, particularly the status of data as an object[45], are almost as difficult as technical understanding of what could comprise a "weapon" in cyberspace, mainly due to the dual-use or omni-use nature of many of the potential subcomponents in a "cyberweapon", and the need for the technical community, researchers, or the private sector to be able to provide security tools for testing. However, if these hurdles can be overcome, the ability to at least agree on a counter-proliferation agreement (similar to the Missile Technology Control Regime or the Nuclear Non Proliferation Treaty) is theoretically possible. Such an agreement would clarify both concepts and capabilities of signatory States, as well as limit the transfer of those capabilities to other actors (including non-State actors).

[44] Alexander Klimburg, "To the GGE and beyond...", UNIDIR Cyber Stability Conference Series, 17 July 2016, Geneva. available at: www.unidir.ch/files/conferences/pdfs/looking-ahead-the-gge-and-beyond-en-1-1173.pdf.

[45] The Second edition of the Tallinn Manual states that, in the opinion of its experts, data is not an object in legal terms (Tallinn Manual at p.127). This view is, however, disputed by other scholars. See for example: Michael J. Adams, "A Warning About Tallinn 2.0 ... Whatever It Says", Lawfare, January 04, 2017, available at: www.lawfareblog.com/warning-about-tallinn-20-%E2%80%A6-whatever-it-says.

If such a treaty neither violated the need of the technical community to have simple and easy access to security testing tools, nor set a dangerous precedent by trying to "outlaw" individual pieces of code globally, then it could arguably provide for a much needed dose of predictability among States.

3.2 Second Basket, Second Committee Issues

The Second Committee of the United Nations General Assembly focuses primarily on economic and financial issues, and has a strong connection to the United Nations Development Programme and the United Nations Economic and Social Council (ECOSOC). The Council is covered by the schedule officers from both the Second and Third Committees. The primary issue on the Committee's agenda is the "digital economy" – an issue predominantly discussed outside of the auspices of the United Nations, by institutions such as the EU, OECD, G20, G7, WEF, to name but a few. The digital economy includes specific issues such as digital trade, e-commerce, infrastructure development, and industry 4.0.

In this context, however, a closer look will be taken at law enforcement cooperation as a potential approach to establish a balance of power. Admittedly, law enforcement cooperation can also be categorised under the First or Third Committee issues. The Budapest Convention on Cybercrime established by the Council of Europe and open to third party members is one of the most authoritative in this context, but has been criticised because it seemingly enforces a Western narrative.[46] In response, Russia has reportedly proposed a draft convention on countering cybercrime and promoting law enforcement cooperation under the auspices of the United Nations, as it apparently believes previous conventions threaten the sovereignty of independent States.[47]

The area of law enforcement cooperation offers some possibilities for pursuing a balance of power approach between States. First, in this context, the power of States is at least partially framed by the second and the third face of power considerations – co-option and conviction of soft power, besides the overall perceived coercive "hard power" strength of its suspected military and intelligence cyber capabilities. Second, a State can relatively easily ramp up its engagement in negotiations in this space, but it will be a credible actor only if it has a strong reputation in general and in the "rule of law" in particular – not necessarily the easiest of all criteria to fulfil. Third, it allows States to address the issue of malicious non-state actors that impact their national security concerns, including, for instance, countering the terrorist use of ICTs. Finally, a law enforcement approach that concentrates on mutual legal assistance treaties (MLATs), rather than specifying specific crimes, does not contradict the legitimizing principle.

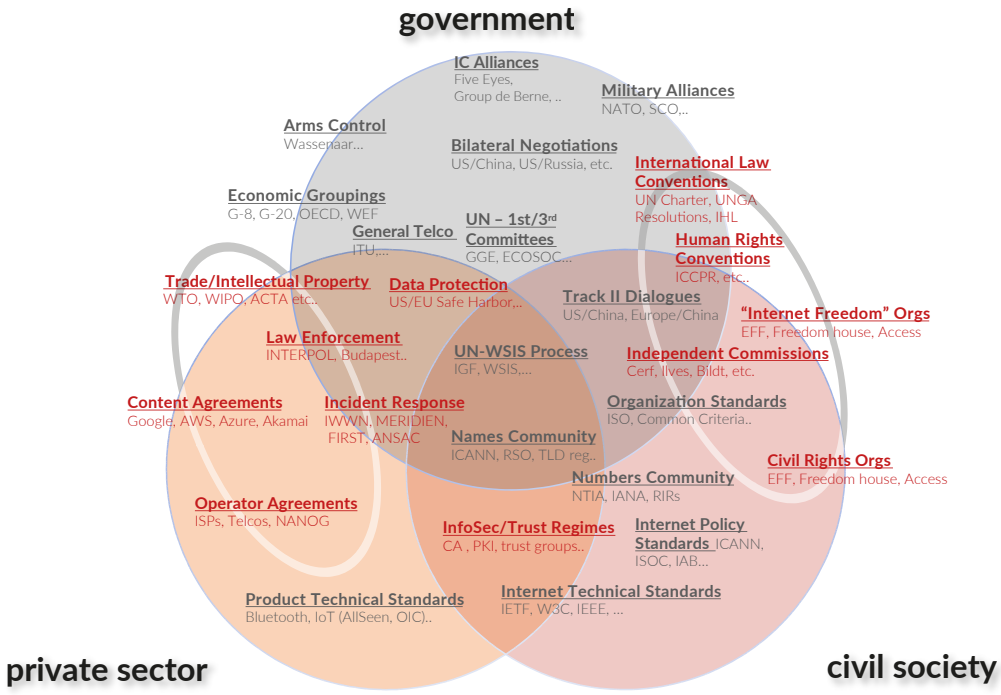
The limitations of the benefits of the law enforcement treaty approach to achieve a balance of power are based upon a simple understanding of what power in cyberspace is. Such a treaty would theoretically have little bearing on a State's ability to conduct offensive cyber operations and therefore would not impact its "hard power" capabilities, unless the government in question clandestinely leverages cybercrime actors to buttress its own governmental capabilities. In the latter case, such a treaty would represent a clear loss for the cybercrime-supporting side, and a number of governments probably do fall into this category, limiting decisively their actual power gains as a well.

A law enforcement approach is theoretically possible and more likely to succeed than the arms control approach described above and the Internet governance approach that will follow below, but it falls short in what it delivers for the balancing of States. Although it does not necessarily address the hard powers of States, it deals with the contentious issue of non-State actors that governments have struggled to manage, and, more importantly, builds confidence among States. A final disclaimer would be that the proposed solutions to "double-bad" issues (illegal in both jurisdictions) can be a slippery slope for increasingly intrusive surveillance measures that the Western like-minded States would not condone.

[46] "Convention on Cybercrime", Council of Europe (2001), European Treaty Series - No 185, available at: www.coe.int/en/web/conventions/full-list/-/conventions/rms/0900001680081561

[47] "Russia Presents Draft UN Convention on Fighting Cyber Crimes in Vienna", Sputnik, May 25, 2017, https://sputniknews.com/science/201705251053959333-russia-un-convention-cybercrimes/ .

Figure 3. The Cyber Regime Complex by Stakeholder Group: "Law Enforcement" & "Civil Rights" clusters marked in red. Source: Alexander Klimburg, 2016.[48]



3.3 Third and Fourth Basket, Third Committee Issues

Third Committee of the United Nations General Assembly focuses the social, humanitarian and cultural issues. Most notably, human rights are discussed within this Committee, and also in other UN institutions, such as the Human Rights Council and UNESCO, as well as outside the UN context: the Council of Europe, EU, OSCE, Freedom Online Coalition (FOC), IGF, WSIS, APC, Human Rights Watch, and many more. The application of international law (including human rights law) has already been established by the United Nations, and a human rights-based approach has been reiterated in many other contexts such as the NetMundial Declaration in 2014. It is, however, unlikely to create a balance of power among States by and of itself as many of the multi-lateralist countries that promote a State-governed Internet through notions such as "cyber sovereignty" remain critical of human rights. Moreover, human rights law governs mainly the relations between governments and their citizens, whereas. Instead, it needs to be incorporated into other approaches.

Finally, there have been several attempts by States to assert power in cyberspace by pushing for a State-led Internet governance approach through the International Telecommunications Union (ITU) of the United Nations. Internet governance is largely treated as a Second Committee issue (primarily through ECOSOC and the Internet Governance Forum) but there are options to connect it to the 3rd Committee as well. The IGF has no formal decision-making power or government policy-making impact, but instead helps to coordinate and facilitate among the different Internet governance constituencies. If the 3rd Committee link to Internet governance can be strengthened, this might also reinforce the notion of a rights-based Internet.

The Internet governance regime complex best represents the complexity of dealing with the larger issues of managing resources and behaviours in cyberspace. It encompasses a wide range of different institutions, from established international organisations like the International Telecommunications Union (ITU)[49] to the

[48] Op. cit. Klimburg, 2016.

[49] The ITU is a United Nations agency established in 1865, whose mission

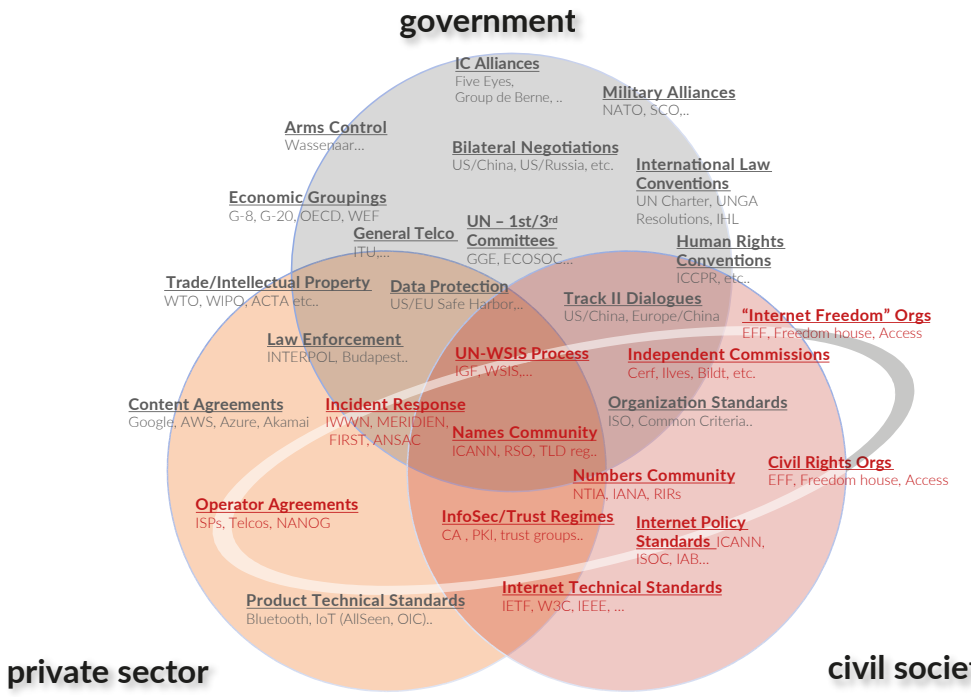
critical Internet Engineering Task Force (IETF)[50] that is characterised by its informal structure, and the non-profit public-benefit corporation known as the Internet Corporation for Assigned Names and Numbers (ICANN)[51]. Most importantly, the Internet governance ecosystem is resolutely representative of the multi-stakeholder approach, with civil society, the private sector and government stakeholders each working more or less equally according to their strengths. As such, it is a "proof" of the legitimizing principle of cyberspace: nothing that is determined about resources and behaviours in cyberspace can be legitimate if it fully violates the basic reality of how the Internet is actually managed.

As such, the only major question of the State's influence on Internet governance was solved by a momentous decision by the Obama administration.

1 October 2016 marked a historic moment, when the US government officially cut the final strings to its influence over ICANN by handing over the IANA function – the management of the root zone file of the Internet – to ICANN in its entirety.[52]

The process of slowly moving the Internet away from government influence was arguably part of the basic US approach to the Internet since as far back as the 1980s. A number of steps under various administrations conformed to this principle – slowly moving the Internet "back into the Internet community" that gave birth to it, even if that community was heavily financed by the US government in its early years.

Figure 4. The Cyber Regime Complex by Stakeholder Group: "Internet governance" cluster marked in red. Source: Alexander Klimburg, 2016.[53]



includes developing technical standards, allocating the radio spectrum, and providing technical assistance and capacity building to developing countries.

[50] The IETF is one of the most important organizations working on Internet protocols and effectively decides much what constitutes the Internet's nervous system; most protocols, such as DNS and BGP. Its mission is to "make the Internet work better" from an engineering point of view. They try to avoid policy and business questions as much as possible, which are mostly managed by the Internet Society.

[51] ICANN is a non-profit public-benefit corporation with the purpose to coordinate at the overall level, the global Internet system of unique identifiers and manage the Internet names and addresses (IANA function) www.icann.org/resources/pages/what-2012-02-25-en,

[52] On 1 October 2016, the contract between ICANN and the United States Department of Commerce National Telecommunications and Information Administration (NTIA) to perform the IANA functions officially expired, handing over the stewardship of IANA functions to the global Internet community. You can read the announcement here: www.icann.org/news/announcement-2016-10-01-en.

[53] Op. cit. Klimburg, 2016.

The commitment of the US government to fully disinvest itself from the last vestiges of direct control over the Internet was given new urgency after the June 2013 Snowden revelations and the significant impact this had on US "soft power", particularly in and through cyberspace. Although it marks an awkward bent in realist thinking that a State would voluntary give up power, the Obama administration made the assessment that sticking to previous political commitments and "releasing" the last shreds of government control over the Internet confirmed to three objectives, namely it reinforced the US soft power when it gave up its first "potentially coercive" face of power, to (i) gain a stronger position in the second face, i.e. in agenda setting or framing, (ii) it confirmed a self-image of the United States as a leader of a "Free Internet", and (iii) it finally reinforced the basic legitimizing principle of the Internet altogether: it is run by the multi-stakeholder approach, and no one government can exercise a hegemonic position on it. Instead, all States enjoy the same relative power. Therefore, the US IANA disinvestment played a significant role in bringing a "balance of power" to the Internet governance domain itself.

The internal balance of power within Internet governance means that it is, in effect, a poor choice for States to advance their power through this approach as it would disrupt the current system and the legitimizing principle. If a State tried to do so at the expense of the multi-stakeholder model, it would conflict with the basic reality of the domain, in which the key technical standard setting bodies, such as the IETF, are resolutely outside of governmental control and due to their voluntary nature cannot be co-opted by it. If a State tried to expand its power while at the same time maintaining the multi-stakeholder model, it would be limited to very small, incremental increases, thus limiting its attractiveness. Restructuring the Internet governance ecosystem to that of an intergovernmental structure is therefore a poor choice for States to seek a different balance of power among States as they already enjoy the same relative power under the current ICANN structure that respects the legitimizing principle of the multi-stakeholder model.

Conclusion: Towards a Basket-Based Approach for Cyberspace

This article set out to assess the application of the balance of power theory to cyberspace to establish international stability and order. It did so by pursuing a more neoliberal interpretation of power. Two conditions of the balance of power theory were applied to three approaches or scenarios that roughly correspond to the first three Committees of the United Nations General Assembly, to see how they could contribute to such a stable environment, leading to the following preliminary observations.

Overall, merit can be found in the realist approach to stability and international order in cyberspace by describing it in terms of compromise and of relative security and relative insecurity. By adopting a neoliberal interpretation of the notion of cyber power, the balance of power theory can be applied to certain aspects of cyberspace. Establishing stability in this environment hinges upon the acceptance of the framework of the international order by all major powers, at least to the extent that no State is so dissatisfied that it expresses it in a revolutionary foreign policy. At least for now, the Internet governance domain enjoys a balance of power among States in accordance with the legitimizing principle. This principle, described as a "recognition of limits" by the State, is construed by the technical reality of the domain inhibiting one party from deciding universally and unilaterally, arguably defined as the multi-stakeholder reality in the context of cyberspace.

However, the condition of an equilibrium of forces that lies at the core of the balance of power theory is currently impossible to establish as it requires States to have a basic understanding of each other's capabilities and therefore a minimum amount of agreed definitions as to what constitutes a "cyberweapon". In this context, compared to the other options, an arms control treaty has most to offer for the balance of power for States in cyberspace. If nearly all difficulties could be overcome, it would clarify those concepts of capabilities that are in much need of more transparency. This transparency can be delivered in the short term through Confidence Building Measures (CBMs), agreements of self-restraint or norms, but those

fall short in terms of visibility, verification, and rigor in the long run compared to the former approach.

Each of the other baskets has its own specific merit, but falls short in establishing a balance of power for States in adherence to the legitimizing principle. Instead, a holistic basket-based approach could serve as an alternative. In a thought piece for the Global Commission on the Stability of Cyberspace, Wolfgang Kleinwächter describes the need, dilemmas, and possibilities of such an approach.[54] Using the context of the "Helsinki Process" of the 1970s as a source of inspiration, Kleinwächter identifies four baskets: (1) cybersecurity, (2) digital economy, (3) human rights, and (4) technology. These correspond to the previously discussed baskets with the addition of "technology". Each basket includes a different constellation of actors and constituencies involved and therefore enjoys different levels of multi-stakeholder and multilateral engagement, as appropriate.

The baskets are not "joined" or organised in a hierarchical fashion. Instead, they are brought together under a decentralised Conference on Security and Cooperation in Cyberspace (CSCC) and connected through a system of liaisons and mechanisms of reciprocal reporting to increase information exchange, cross-fertilisation, and eventually, more coherence across these topics. Like its historical precedent, each basket is negotiated individually, but remains interconnected with the others, allowing asymmetric compromises in the negotiation processes – as the British Foreign Minister argued in 1972, "if we don't lay eggs in the third basket, there will be none in the other ones either". Ideally, over time, the actions of States would balance out across all baskets, enabling not only information exchange but also a more concerted level of negotiation between States. The Conference would aim at drafting a "Final Act on Security and Cooperation in Cyberspace" (FASCC), legally non-binding commitments from governments, the private sector, civil society and the technical community.

[54] Wolfgang Kleinwächter, "Towards a Holistic approach for Internet Related Public Policy Making: Can the Helsinki Process of the 1970s be a Source of Inspiration to Enhance Stability in Cyberspace?", 2018, published by the Global Commission on the Stability of Cyberspace, available at: https://cyberstability.org/wp-content/uploads/2018/02/GCSC_Kleinwachter-Thought-Piece-2018-1.pdf.

A basket-based model inspired by the Helsinki Process could create an environment in which all major players can expand their foreign policy interests in the respective baskets, while leaving room for others to do the same, leading to a more stable situation whereby all States are equally (dis)satisfied and at the same time respect the legitimizing principle of a multi-stakeholder reality in cyberspace. No matter how likely its success, it needs to be seen as a collaborative effort where progress towards stability can be made on several fronts.

The basket-based approach is obviously just one approach that need not frame a "final answer" to the overarching problem of balancing States' interests in cyberspace. But it may form a beginning. ■

LOOKING INTO THE CYBERFUTURE THROUGH THE EYES OF **YOUNG LEADERS**

The Kosciuszko Institute is launching a new initiative addressed to young, ambitious and visionary students interested in strategic and interdisciplinary aspects of cybersecurity from most renowned academic institutions of the entire world. Our aim is to create a coalition of educational institutions that will patronize the quest for young leaders aware of high significance of cyber challenges and help them boost their careers in the domain.

WHAT?

We warmly invite MA and PhD students to take part in the CALL FOR PAPERS on challenges in cyberspace within such domains as international relations, economy, national security, defence, etc.

WHEN?

The IV European Cybersecurity Forum – CYBERSEC will be held on **8 - 9 OCTOBER 2018** in Krakow, Poland.

HOW?

The universities willing to take part in the consortium are responsible for sharing the information about the call for papers with their students. These universities' logos will be exposed while promoting the endeavour.
The papers shall be sent till the end of June to **editor@cybersecforum.eu**.
Please find publication guidelines attached.

WHY?

Once a year, the mesmerizing city of Krakow becomes the European centre for strategic discussions on cybersecurity, a place of inspiring debates, presentations and informal conversations.
Authors of 3 best papers will be invited to take part in the specially dedicated panel discussion entitled *Young Cybersecurity Leaders looking Ahead* during the IV European Cybersecurity Forum – CYBERSEC.
The panel will be held under the auspices of the overmentioned coalition of universities.
CYBERSEC is a public policy conference dedicated to the pivotal aspects of cyberspace and cybersecurity. CYBERSEC gathers more than 1,000 participants from around the world, including political decision-makers, diplomats, experts, business leaders and academic researchers.
Winners will be granted:
- VIP pass for the whole conference including travel & accommodation and unlimited networking opportunities,
- Invitation for afterhours events, e.g. CYBERSEC Banquet,
- Publication of their articles in the **European Cybersecurity Journal.**

CYBERSEC
YOUNG LEADERS

INTERVIEW WITH PROFESSOR PAUL CORNISH

PROF. PAUL CORNISH
Professor Paul Cornish was educated at the University of St Andrews, the London School of Economics, the Royal Military Academy Sandhurst and the University of Cambridge. He served in the British Army and the Foreign and Commonwealth Office and has worked in UK research institutes and universities: Chatham House; the UK Defence Academy; the Centre for Defence Studies (King's College London); the RAND Corporation (Europe); and the Universities of Cambridge, Bath and Exeter. His work covers international security futures, national strategy, cyber security, arms control, the ethics of conflict, and civil-military relations.
He is Chief Strategist at Cityforum Public Policy Analysis Ltd, Associate Director of Oxford University's Global Cyber Security Capacity Centre, and Professorial Fellow in Cyber Security at the Australian National University's National Security College (2017-2018). He has participated in UK-China Track 1.5 discussions on cyber security since 2013 and advises an OSCE project on confidence-building measures in cyberspace. Cornish's most recent book is 2020: World of War, published by Hodder & Stoughton in July 2017. He is editor of the Oxford Handbook of Cyber Security, to be published by Oxford University Press in 2018.

In your article entitled 'Governing Cyberspace through Constructive Ambiguity', you claim that people have a natural instinct to oversee and regulate cyberspace. It seems that currently we observe plenty of voices that support this point of view. What is your stand on that? Do we need regulation? If yes, to what extent and in which areas? What are the obstacles?

I find it difficult to think of any aspect of human society where regulation does not play some role. Human beings are social animals and a distinctive feature of human society is that its members either inherit or agree upon a set of rules, standards, customs etc. to which they adhere. These rules and customs contribute to the cohesiveness and durability of society. If there were no rules or codes of conduct then it would be – at best – a very loosely formed society and probably not very durable. Equally, if it were a society where adherence to the rules was optional, then it might be difficult to define the basis upon which that society had been formed. Why bother with society at all, in that case?

So far so good. But it is important, I believe, to be careful about our instinct to oversee and to regulate. Regulation must be *for* something – it cannot be an end in itself. And regulation must also be subject to periodic critique – it must be made accountable to those whose lives it affects. Perhaps you could say, in other words, that regulation is fine – as long as it's properly regulated. And another point to bear in mind is that regulation isn't simply *descriptive*, it's also *purposive* – or *normative*, if you prefer. It's not simply a matter of society writing down the 'rules of the road', so to speak. It's also a matter of society knowing where it wants the road to lead.

In Governing Cyberspace through Constructive Ambiguity, I wrote about what I called a 'regulatory impulse', arguing that this instinct to oversee and to regulate is particularly strong where the Internet is concerned. The global ICT infrastructure is a technological construct. We – humanity – made this thing that affects so much of our lives, and so it seems both appropriate and necessary to ensure that it meets our needs and aspirations. It's at this point that the regulatory impulse leads off in several directions, not all of them compatible. A minimalist, or technical

approach to regulation would be to do whatever needs to be done to maintain a well-ordered, disinterested global information network – and nothing more. A more ambitious, or libertarian approach would be to argue that the Internet should be governed by self-regulation – and nothing else. And perhaps the most ambitious, or emancipatory approach would be to argue that the global ICT infrastructure offers a revolutionary opportunity for human freedom and fulfilment and that the purpose of regulation should therefore be to persuade or coerce governments and corporations around the world to improve their behaviour – and nothing less.

> “ Although I have argued for a cautious approach, I accept that we cannot afford to hang about and wait for perfect regulatory solutions to emerge.

In one way or another, all three of these approaches to regulation seem to me, in principle, to be valid and persuasive. And this explains why, as you suggest, there are so many voices advocating regulation, often for very different reasons. Where do I stand? As I've suggested, I think we *want* regulation – it's in our DNA as social animals – and we *need* it too, because as much as the Internet presents us with great opportunities, it also confronts us with challenges and threats. My own preference would be to start fairly small and make incremental progress, rather than set out in pursuit of some grand regulatory vision only to see it falter. In the first place, I'd argue for regulation in areas where its benefits can be most obviously felt, such as cross-border police cooperation, CERT-CERT information exchanges and operational assistance, and the assurance of financial transactions, particularly where social and economic development assistance is concerned.

The most obvious obstacle to all of this is time. Although I have argued for a cautious approach, I accept that we cannot afford to hang about and wait for perfect regulatory solutions to emerge. Regulation has to be responsive and agile, not least because communication and computing technology continue to develop at an extraordinary rate and in extraordinary breadth. Another obstacle is inconsistency – any regulatory system is only as good as its weakest, least committed component. And the final obstacle is those less scrupulous actors who see regulation as a loss of initiative on the part of its high-minded advocates, and an opportunity for them to exploit.

The Internet of Things emerges as a critical area of interest to policymakers and is seen as a true game-changer in the area of cybersecurity. With your team, you have carried out a study to support a process for policy feedback that will inform the development and adoption of the IoT in the UK. What are the most surprising and the most interesting conclusions?

I'm struck – as we all must be – by the rate of growth of this phenomenon. By one reputable account, by 2020 there could be as many as 50 billion 'things' connected to the Internet, each generating its own telemetry; some halve that estimate, others double it. Some of these connections (using WiFi to open and close curtains, for example), look rather trivial but others, such as personal health monitoring, are critically important. How much of this digital ecosystem needs to be made secure from hackers and botnetters – all of it? How do we go about it? Why hasn't it been done already, prior to installation? And what about the telemetry – who owns all the data?

With former colleagues at RAND Europe, I co-authored a report entitled *Accelerating the Internet of Things in the UK: Using Policy to Support Practice*, published in 2016. The core of our approach was to say that if the IoT policy is to have the credibility it needs, then public attitudes to, and familiarity with the IoT must feed into the policy-making process, alongside other voices from within government, from the private sector and from innovators in academia and industry. Perhaps the most surprising conclusion of the survey was that environmental sustainability and organisational efficiency were seen to be the most significant benefits of the IoT. But the most interesting conclusion, in my view, was that where the IoT is concerned, quality matters more than quantity. Rather than see the IoT simply as a huge

investment opportunity and a boost to the national economy, governments (in the UK and elsewhere) should instead use public money to stabilise the IoT through expenditure on training and education and on multi--stakeholder collaboration (between academia, government and the private sector, for example).

Last September, the European Commission proposed the so-called Cybersecurity Package – a set of numerous initiatives that aim to enhance cybersecurity in Europe. Among others, the Commission plans to launch a new European certification scheme, and this particular idea seems to evoke powerful emotions. What is your stand on that? Do you agree with those who are saying that nation-states have to have possibilities and tools to introduce their own certifications, at least for their most critical systems?

The European Commission has proposed an EU-wide cybersecurity certification scheme to be led by the EU Agency for Network and Information Security (ENISA). The initiative is intended to promote cybersecurity by certifying that ICT products and services are compliant with certain EU-wide, standardised cybersecurity requirements. The merit of a pan-EU approach, it is claimed, is that individual companies would no longer need to seek certification in different member states individually, where each state might have its own testing methodology and might insist on particular certification procedures. The initiative would be voluntary (at least in the first instance) and it is here that the first criticism arises. If certification is voluntary, then the initiative is neither one thing nor another and there can be little or no hope of establishing comprehensive EU-wide participation. It seems unlikely to me that EU governments would be willing to drop their own, more or less rigorous requirements for ICT certification without a viable and effective (EU) alternative available which would make their national efforts unnecessary. For their part, companies might then see little point in undertaking an additional, time-consuming and expensive EU certification process while still having to certify at the national level.

A broader and deeper criticism concerns the competence of the European Commission in matters of national security. The purpose of the Commission's 2015 Digital Single Market Strategy (DSM) has been described as 'tearing down regulatory walls and moving from 28 national markets to one single one'. More specifically, the Commission's mid-term review of the DSM notes that 'the lack of interoperable solutions (technical specifications), practices (process specifications) and EU-wide mechanisms of certification was [*sic*] identified as one of the gaps affecting the single market in cybersecurity.' [Emphasis added] Clearly, the Commission considers that the goal of the DSM legitimises its interest in certification and cybersecurity more broadly. But cybersecurity is not solely an industrial/commercial matter, or a question of achieving openness and efficiency in the market. Cybersecurity is also about *national* security, and it is at this point – at least in the mind of some EU governments – that the argument for EU-wide market efficiency gives way to the paramount requirement for effective national security. Although Article 346 of the EU Treaty of Lisbon does not explicitly rule out the European Commission's involvement in this area, along with other measures in the treaty Article 346 does at least express member states' persistent wish to limit the extension of the European Commission's competence into matters of national security (including cybersecurity); matters which remain the preserve of governments.

> "What matters most – the Digital Single Market or national security?

What is my position? There would seem to be two, not entirely disconnected motives in play: the further development of the DSM on the one hand and the promotion of cybersecurity on the other. If a regulatory or standardisation initiative cannot satisfy both demands and is unlikely, as a voluntary measure, to include all members of the EU (thereby making national standardisation efforts superfluous), then we have a choice to make. What matters most – the DSM or national security? I consider security to be necessary to the successful functioning of any society. And given my view that any regulatory device must be made accountable to those it affects and must be subject to periodic critique, I'm pushed in the direction of national certification, at least for the time being and until circumstances change.

You are the Co-Director of Oxford University's Global Cyber Security Capacity Centre. Could you please tell us a little bit more about the Centre? What are its goals, mission and planned initiatives?

Founded in 2013 with the support of the UK Foreign and Commonwealth Office, the Global Cyber Security Capacity Centre at the University of Oxford is a leading research centre and a global knowledge resource for effective cybersecurity capacity-building at national and regional levels. My colleagues and I have created a systematic model with which countries can assess the maturity of their cybersecurity capacity: the Cybersecurity Capacity Maturity Model (CMM). The CMM assesses cybersecurity capacity in terms of five 'Dimensions': Cybersecurity Policy and Strategy; Cyber Culture and Society; Cybersecurity Education, Training and Skills; Legal and Regulatory Frameworks; and Standards, Organisations and Technologies. In each Dimension (and sub-Dimension or 'Factor'), a set of indicators are used to gauge cybersecurity maturity along a five-stage spectrum: Start-up, Formative, Established, Strategic, and Dynamic.

The CMM is emphatically not a cybersecurity capacity ranking exercise of some sort. Instead, we offer governments a guided self-assessment, the results of which are theirs, not ours. The Oxford Model (as it has also become known internationally) enables governments to identify their existing and potential capacity in cybersecurity. Based on that assessment, governments will be in the optimal position to assess risk, identify priorities and plan their investments and strategies for developing national cybersecurity capacity accordingly.

We have been very vigorous in expanding the reach of the Oxford Model, gathering experience, knowledge and data across Latin America, the Caribbean, Europe, Asia and Africa. So far, over 60 countries have undergone the CMM assessment, whether undertaken directly by the GCSCC research staff or indirectly under the auspices of a GCSCC stakeholder organisation. We work very closely with several international bodies – the World Bank, the International Telecommunication Organisation, the Organisation of American States and the Commonwealth Telecommunications Organisation – and we have benefited from the close support and collaboration of the governments of the Netherlands and Norway, as well as several others.

Our planned initiatives include the completion of our second major project – the development of a model for national cyber harm assessment (CHM) and its full integration into the CMM methodology. We intend to use the CMM/CHM twin-track as the basis for intergovernmental and regional confidence-building measures in cyberspace. We have agreed a major strategic partnership with the Oceania Cyber Security Centre in Melbourne, Australia and we intend to develop further high-level partnerships around the world. We are expanding the scope and availability of our Portal for capacity-building expertise and we plan to develop work on preventive cyber diplomacy. We have recently launched a project to strengthen our ties with European governments and with the European Union and NATO, and we have a very busy CMM assessment schedule into 2018 and beyond. ■

Questions by Dr Joanna Świątkowska

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.

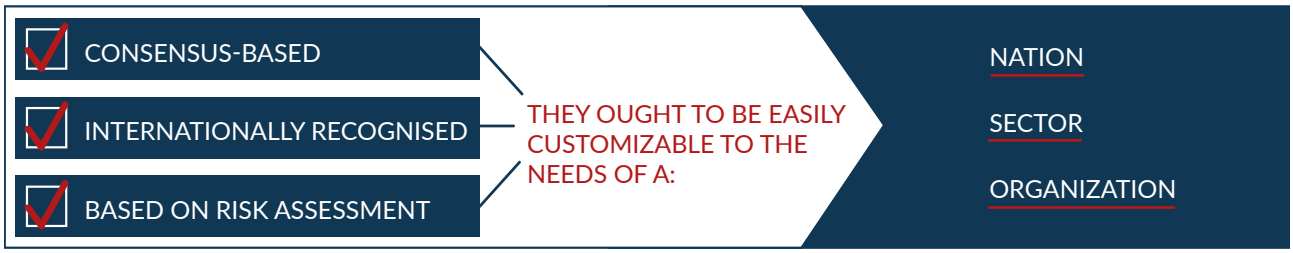
Governments must take the lead in the quest for cyber trust.

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

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.

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:

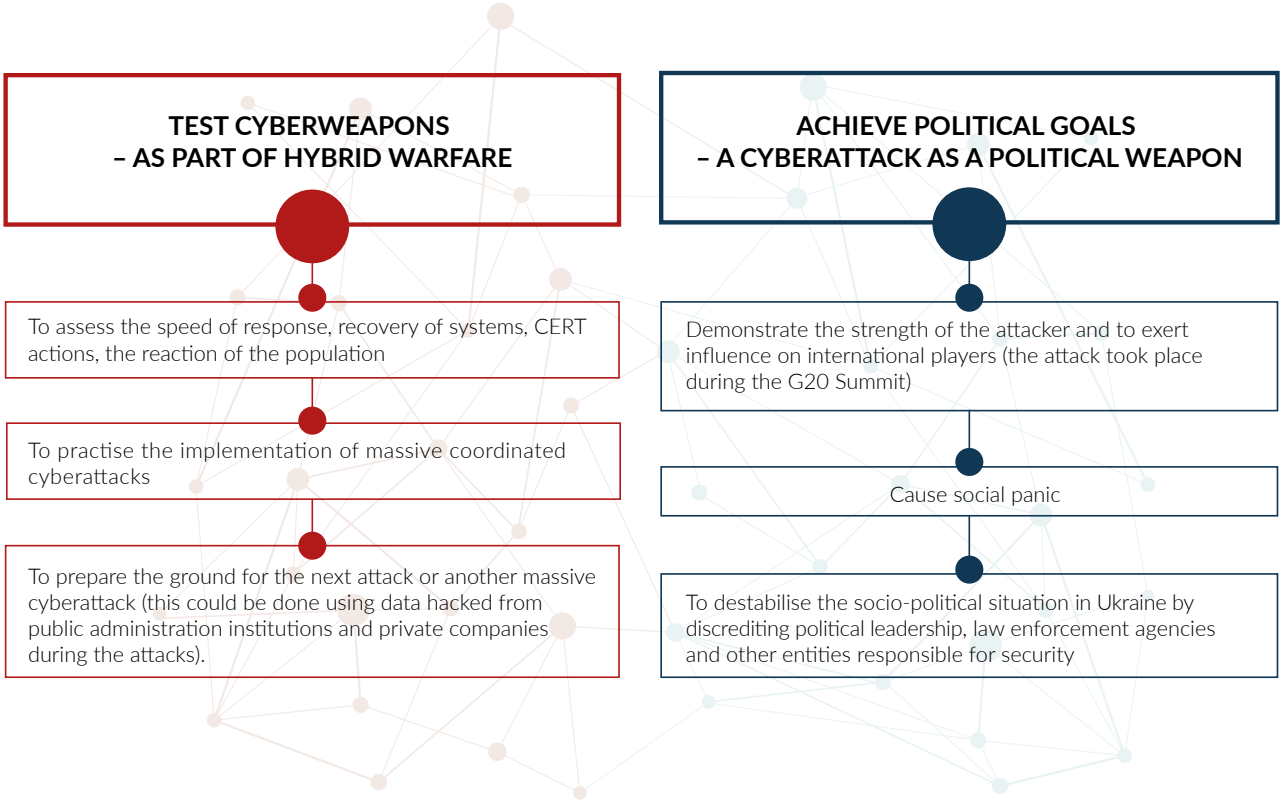
- Conducting a comprehensive risk assessment that reaches beyond technology.
- Having the right legal framework in place to make sure that systems have sufficient protection (e.g. recognise i-voting systems as critical infrastructure).
- Providing constant testing, feedback and improvement (to be done 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 STRENGHTEN NATO'S CYBER DEFENCE

IIn 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.

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

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.

TRUST

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).

DECENTRALISATION

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.

*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

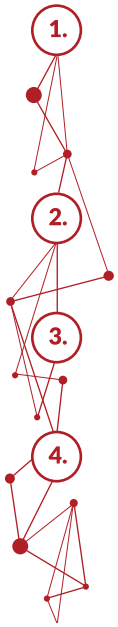
We should not assume a priori that a new treaty will resolve all the problems that we currently observe. Development of voluntary cybersecurity norms should be encouraged as an inclusive process involving multiple stakeholders (as many states as possible, but also global non-state actors, such as IOs, 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:*



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.

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

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.

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.

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:

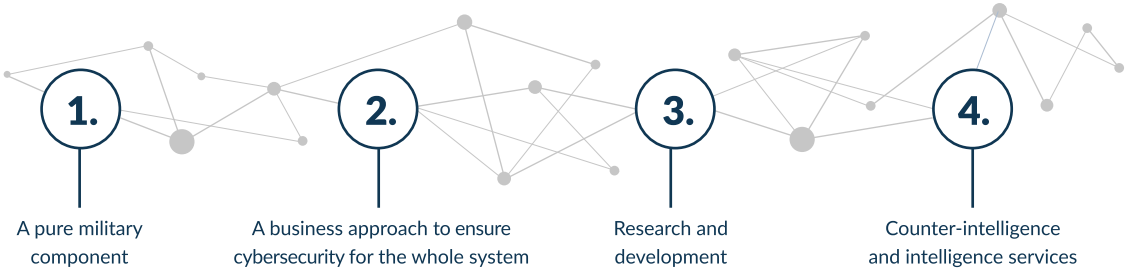
INTELLIGENCE CYBER OPERATIONS | **SPECIAL CYBER OPERATIONS** | **TACTICAL CYBER OPERATIONS**

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.

1. ENCRYPT CRITICAL INFORMATION
2. KNOW AND CONTROL YOUR OWN PERSONNEL
3. KNOW, MONITOR AND CONTROL INFORMATION THAT COMES OUT OF YOUR ORGANISATION – DEFEND AGAINST INSIDER THREATS
4. DOMINATE THE ELECTROMAGNETIC SPECTRUM

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.

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 it 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.

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.

CYBERSECURITY OF SMART CITIES

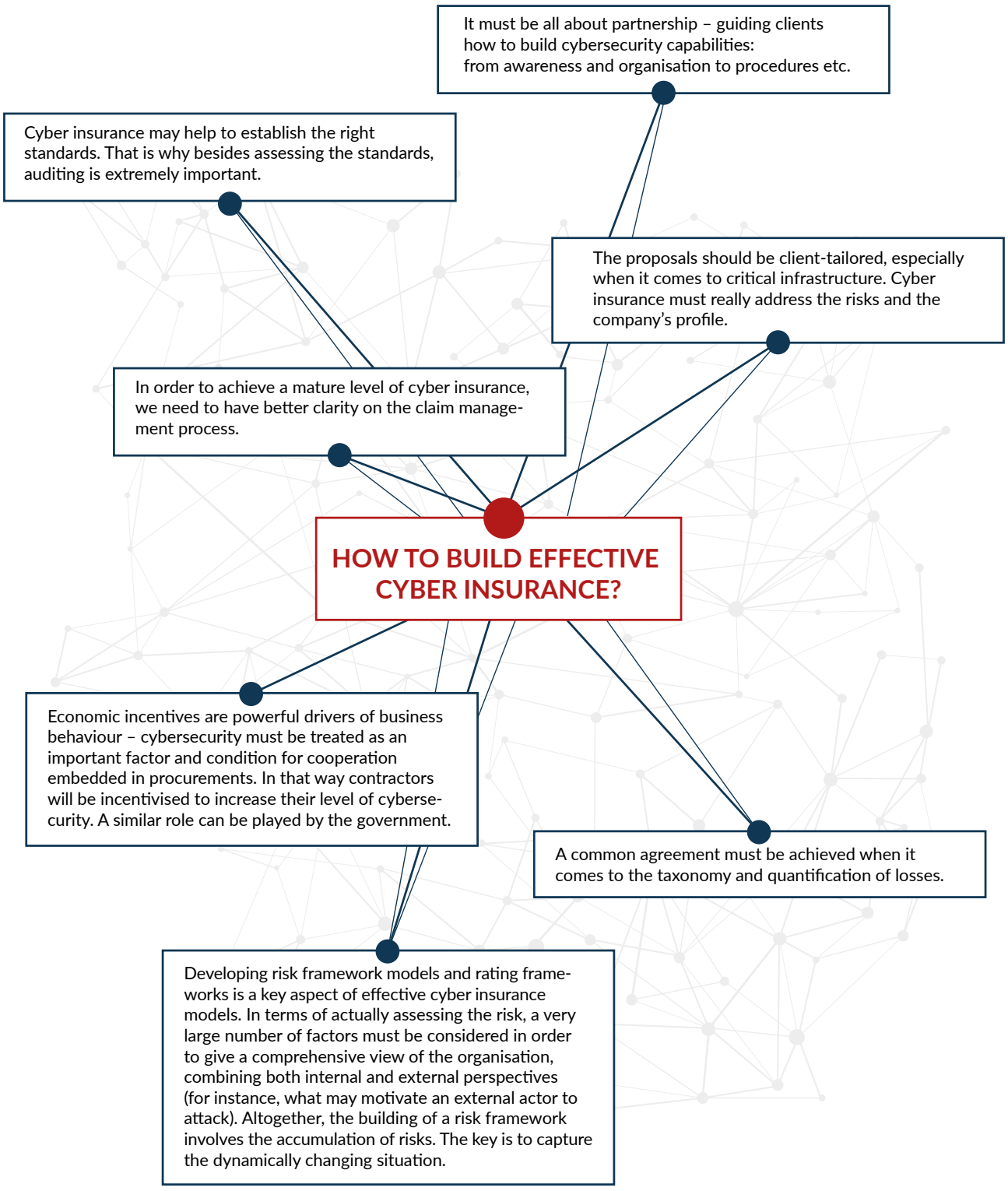
- The complex landscape of IT and cybersecurity vendors using various products within one ecosystem makes it harder to ensure cybersecurity. This issue requires further consideration.
- It is important to have rules imposing that people can have access to resources and information relevant from the point 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

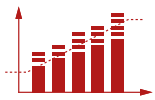
Providing effective cyber insurance is much more than simply insuring – it is about building cyber risk governance with a strong component of the whole culture around cybersecurity.



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.

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:

1. Better quantification of network risk is needed
2. Increased automation of detection and response
3. Cross-sector disaster simulations to provide much needed data
4. Solid research on IoT endpoints

*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

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

Effective SOCs 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. ■

CYBERSEC 2017

IN NUMBERS

1
Emerging Public Policy Challenge

2
Days of Thought Provoking Debates

>600
Articles about CYBERSEC

>90
Accredited Journalists

1,2 MLN
EUR Advertising Value Equivalent

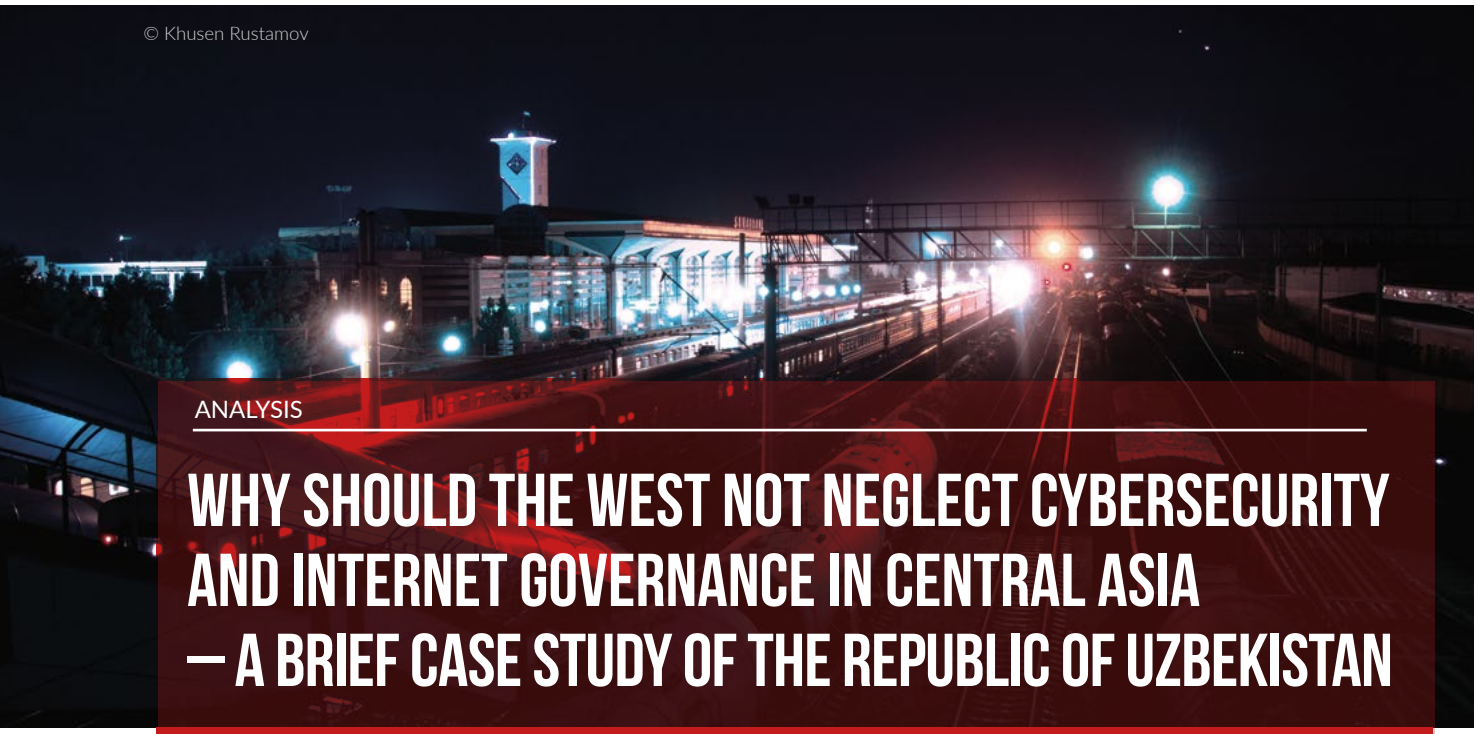
>150
Speakers

4
Thematic Streams

>100K
Twitter Impressions

>220
Individual companies represented

>100
Partners



ANALYSIS

WHY SHOULD THE WEST NOT NEGLECT CYBERSECURITY AND INTERNET GOVERNANCE IN CENTRAL ASIA – A BRIEF CASE STUDY OF THE REPUBLIC OF UZBEKISTAN

MAGDALENA SZWIEC
graduated with a Master's degree in international security. Previously she worked as Project Manager and Junior Research Fellow at The Kosciuszko Institute in Poland, where she focused on national and international aspects of cyber defence. She currently works at NATO Headquarters in Europe (SHAPE).

In the 21st century realm, the role of the Internet in sustainable and equitable development is undeniable. Accordingly, in order to be socially beneficial, the Internet needs to be properly governed and secure. Ensuring these aspects may improve access to healthcare and education, conservation and fair distribution of resources, and strengthening society's participation in the decision-making processes and the rule of law.

Uzbekistan, while officially a democratic, constitutional republic, was in fact ruled by the authoritarian regime of President Islam Karimov since gaining independence from the USRR in 1991. Last year after 25 years in power, Karimov died and his place was taken by Prime Minister Shavkat Mirziyoyev. This peaceful shift of power and the first few months of new presidency have brought hope for liberalisation[1]. Nevertheless, the new president pledged to continue the legacy of his predecessor, which puts in question potential improvements in the areas of human rights and civil liberties.

The situation in Uzbekistan matters for several reasons – firstly, the country enjoys a strategic location that has attracted the interest of many foreign states throughout its history[2], as it is rich in natural resources such as oil, gas and gold. It has the largest army in the region and the biggest population of all Central Asian countries. Above all, it shares our security challenges: border security, religious extremism and radicalisation, drug trafficking, corruption. Today, a new threat has emerged – crime involving high technology and the Internet.

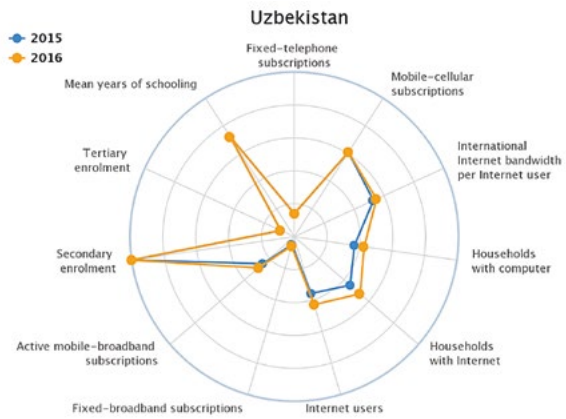
[1] On May 10 2017, United Nations High Commissioner for Human Rights Zeid Ra'ad Al Hussein became the first such commissioner to visit Uzbekistan.

[2] In 2001, the government in Tashkent allowed USA to use its air bases in support of military action in Afghanistan. The agreement was cancelled after Washington's criticism of the Uzbek government's human rights record.

Access to ICT in Uzbekistan

- Fixed-telephone subscriptions (per 100 inhabitants): 8.44
- Mobile-cellular telephone subscriptions (per 100 inhabitants): 73.32
- International Internet bandwidth per Internet user (Bit/s): 2,075.36
- Percentage of households with computer: 43.20
- Percentage of households with Internet access: 52.60
- Percentage of individuals using the Internet: 42.80
- Fixed (wired)-broadband subscriptions (per 100 inhabitants): 3.57
- Active mobile-broadband subscriptions (per 100 inhabitants): 28.69[3]

Figure 1. ICT Development Index's score for Uzbekistan[4]



Organisational and Administrative Aspects

Ministry for Development of Information Technologies and Communications (MININFOCOM)

In 2015, President Karimov signed a decree "On creation of the Ministry for Development of Information Technologies and Communications of the Republic of Uzbekistan". The spectrum of the responsibilities covers the implementation of unified state systems, comprehensive programs and policies in the field of ICT. It also includes the improvement and modernisation of national ICT infrastructure; coordination, monitoring, evaluation, and controlling of the ministries, departments, companies, associations, and public authorities in the field of information. Beyond the aforementioned areas, the ministry is responsible for R&D in the field of ICT; promoting and assisting in the development of domestic production and domestic market of competitive software and services; and international cooperation.[5]

Information Security Center

The Center has been established based on the Resolution of the Cabinet of Ministers in 2013 and operates as a part of MININFOCOM. Under its main responsibilities fall the administration and security of information systems; resources and databases of the "E-Government" system, assistance in the development and implementation of information systems and resources; information security policy of the state bodies; analysing, monitoring, and responding to threats to information systems; developing proposals to improve regulatory and legal framework; cooperation with telecommunication network operators and providers; collaboration with law enforcement agencies and development of international cooperation.[6]

Computerization and Information Technologies Development Center

The Center's main activities focus on ICT introduction and implementation in education; development of a national Internet network; automation of administrative and business processes of organisations. In 2005, UZ-CERT has been created within the Center's structure.[7]

Besides the existing bodies, Uzbekistan is still lacking elements essential to create a national cybersecurity framework. The situation is similar in the legislative domain. Some laws concerning cyberspace have been enacted, for example the Law on Informatisation,

[3] Op.cit. ICT Development Index 2016

[4] Source: ICT Development Index 2016, [online] http://www.itu.int/net4/ITU-D/idi/2016/#idi2016countrycard-tab&UZB, (access: 14.06.2017).

[5] Ministry for the Development of Information Technologies and Communications, [online] http://www.ccitt.uz/en, (access: 14.06.2017).

[6] [online] https://infosec.uz/en/about/functions-tasks/ (access: 14.06.2017).

[7] UZININFOCOM, [online] http://uzinfocom.uz/en/page/show?alias=start_here, (access: 14.06.2017).

Law on Communication, Law on Electronic Commerce, Law on Legal Protection of Software and Databases, Law on Telecommunications, Law on Principles and Guarantees of Freedom of Information, Law on Protection of Information in the Automated Banking System.[8] Particular amendments have occurred in Uzbekistan's Criminal Code. The changes focused on unauthorised access to information networks or illegal data acquisition. New regulations covered also illegal change, loss, withdrawal or deletion of information and production of computer viruses or programs. All of these offences have been classified as punishable.

Controversies Around Internet Freedom

Despite constitutional guarantees, freedom of speech and press are actually restricted. Although censorship was abolished in 2002, the Uzbek government still controls major media outlets, systematically blocks websites that contain content critical of its activities, as well as mainstream news, information, and social media sites based outside the country.

In 2014, the government amended the Law on Informatisation, which brought bloggers and online news providers, including freelance citizen journalists, under state regulation subject to content removal requirements. According to the legislation's broad definition, any person may qualify as a blogger by disseminating information "of socio-political, socio-economic and other character" to the public through a website. The same law entitles a dedicated governmental body to limit access to websites that do not comply.[9]

Additionally, the abovementioned Ministry for Development of Information Technologies and Communications regulates web content in order to prevent the Internet's "negative influence on the public consciousness of citizens, in particular of young people." In other words, monitor and filtrate the contents of websites.

Conclusions

The situation in Uzbekistan might not be improving any time soon, but with the use of available tools the international community can help establish a safe and democratic cyber environment. The spectrum of available instruments is broad and could be introduced by for instance:

- promoting cyber capacity building,
- developing a broader understanding of the country-specific approach to cybersecurity,
- enhancing the ability to counter cyberthreats,
- introducing internationally recognised good practices,
- sharing experiences in cyber policies and strategies building.

Overall, by improving Internet accessibility and freedom, the Uzbek society would make a step towards liberal democracy and socio-economic development. ■

[8] Cyberwellness Profile Republic of Uzbekistan, [online] https://www.itu.int/en/ITUD/Cybersecurity/Documents/Country_Profiles/Uzbekistan.pdf, (access: 13.06.2017)

9 *New restrictions in Uzbekistan further limit free expression on Internet, OSCE Representative says*, [online] http://www.osce.org/fom/123275, (access: 14.06.2017).


GET CYBER READY!
CYBERSEC
EXPO 2019
17-18.01.2019
GlobalEXPO Warsaw
CYBERSEC

INTERVIEW WITH GRZEGORZ JASIULEWICZ

GRZEGORZ JASIULEWICZ
Grzegorz is an experienced cybersecurity manager who works for Alior Bank, one of the most innovative banks in Europe. He has the privilege to lead one of the best cybersecurity teams in the Polish banking sector. He manages the team of about 40 highly qualified and open minded experts who are responsible for the day-to-day security of Alior Bank in such areas as IT security, online transaction security, fraud detection, card payment security and physical security.
Before joining Alior Bank, he led the teams of IT Security experts at Deutsche Bank PBC S.A., Orange Poland and he also served in the Polish Army. He graduated from the Faculty of Electronics at the Military University of Technology in Warsaw. He also completed post-graduate studies in the field of risk management in financial institutions at the Warsaw School of Economics (SGH), social psychology at the SWPS University of Social Sciences and Humanities and Master Of Business Administration for IT at the Kozminski University.

Banks have a new weapon against cybercrime. Bank accounts get secure: How you use your keyboard or mouse can protect your bank account from cybercrime. Alior Bank experts are planning to implement innovative solutions.

Banks used to protect money in the vault from theft. This is not the main concern any more, is it?

Today, money is mainly virtual. It circulates in electronic channels, so the challenge is different.

Banks boast of security measures and yet media reports often bring alarming news: a bank website has been forged, bank security breached. Are we safe with our money in electronic banking?

Money in the bank is nothing if not safe. Both the customers and the Polish Financial Supervision Authority expect to invest in and improve security measures continuously. If you look at statistics, less than one online transaction in Poland in a million is unauthorised. This is a minute fraction.

Unauthorised means what exactly?

In a nutshell, a transaction ordered by a criminal. How can it be done? There are many ways. One way is to use social engineering. A criminal calls a customer and pretends to be a bank or a bank's lawyer. There has been an incident, we need to check your identity. Careless users may disclose data without giving it a second thought: logins, passwords, OTPs.

People disclose such data on the phone to a stranger?

Sometimes they do. It is a social engineering method frequently used by criminals. But there is a host of technical means to take control of a customer's computer. The criminal can then control the screen.

Someone knows my bank account number but so what? They can pay money into it, nothing more. It's the same if they know my bank login and password. I still have to confirm each transaction with an OTP.

Now I know how to steal your money... You give me your login and password and I call you and say, "Mr Customer, we are testing our security system. You will be sent a text message with a code. Please read it to me." And I can make a transaction with your login and password. You might

think there is no connection. What's wrong with revealing a text message code? But I already have your login and password. I could have got hold of them months ago. After all, customers hardly ever change their passwords.

What else could happen if someone gets my authorisation code?

I don't want to give anyone ideas. But customers must remember that they are the only ones who should know the password. Never disclose it to anyone. It's the same with authorisation codes. Never read them to anyone on the phone or forward in a text message. You may only enter a code on the bank's website. But first remember to read the authorisation text carefully.

Customers often only look at the six digits of the authorisation code. That is not enough! Why? A criminal who has taken control of your computer could display a fake page on the screen. Meanwhile, having access to your account, they could make transactions by prompting you to enter the OTP on the screen, seemingly to confirm your identity. If you only read the code and not the whole message, you may confirm a criminal transaction thinking that you're confirming your identity.

I'm starting to think that logging into my account on the computer is a major risk...

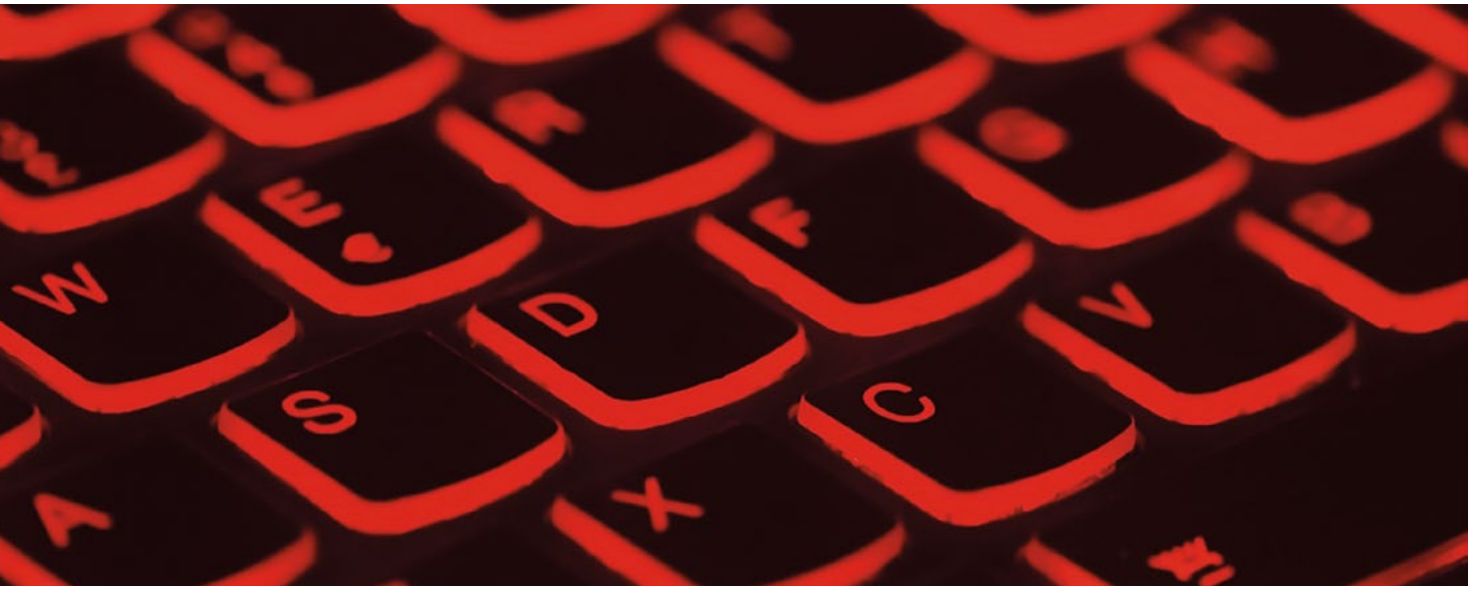
No, it isn't, just be careful. For comparison, the number of cybercrimes in Poland is 20-30 times lower than the number of car accidents. After all, we keep on driving. Banking security is much like traffic security. It is largely up to the driver's behaviour whether they cause an accident or not. It's the same with a banking customer. If you log in on unknown devices or computers in an internet café or hotel, the risk that someone could break into your account is much bigger. This is why we encourage all customers to read the security rules published on the bank's website. It's just as important as knowing the traffic code when you're driving.

What if someone steals your money and it's your fault?

Contact the bank's call centre immediately. We have competent people who know what to do. Alior Bank responds to customers' security calls 24/7. If you react quickly, there is a big chance that you won't lose your money. Even if the transfer has gone out, it will have to come to another bank. Banks co-operate in security matters so the money could be sent back.

What if I don't discover the scam until the next day?

Sometimes money is withdrawn from an ATM minutes after the transaction, sometimes it sits in another bank account for days. It's not like there are any fixed rules. But each time there is a theft or attempted theft, you must contact the bank immediately.



My friend has had money withdrawn from her account in Asia while she was at work in Warsaw. Someone must have scanned her card in Warsaw. Can she get her money back?

The bank will certainly look into it. In most cases, customers get their money back.

Since there are so many cyberthreats, you must be working on new security measures.

Certainly. We are working on biometric security, including face and voice biometrics. We want to offer a security package where customers may select the preferred online security options. It's not a good idea to force all customers to use the same security measures, for instance by entering a masked password. We want our customers to have a choice.

And then there are security systems which remain invisible to customers. We have a number of mechanisms in place to identify unauthorised transactions by capturing atypical customer behaviour.

You mean, when a client never goes to Africa but suddenly they are transferring money to Africa or withdrawing cash from an African ATM?

That is the most typical example. We want to go further and focus on IT anomalies, behavioural biometrics which analyses how customers use the computer, for instance the speed of typing on the keyboard or navigating on the screen. These are idiosyncratic patterns of behaviour. Criminals cannot emulate you even if they take control of your computer. With such controls, we can secure bank accounts against unauthorised transactions.

What if my wife goes on my computer and uses my login to order a financial transaction?

We can detect that too and stop the attempt online, because to us it will look atypical. ■

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