Addressing the elephant in the room: cyber intelligence and international security

Broeders, D.W.J.

Prof. dr. Dennis Broeders

Addressing the elephant in the room. Cyber intelligence and international security.

Universiteit Leiden

Addressing the elephant in the room. Cyber intelligence and international security.

Inaugural lecture given by

Prof. dr. Dennis Broeders

On the acceptance of his position as professor of

Global Security and Technology

at Leiden University

on Friday March 31, 2023

Universiteit Leiden

Esteemed Rector Magnificus,
Dear colleagues, friends and family,

What do we talk about when we talk about Cyber intelligence operations?
In the 1983 movie *War Games* a young kid hacks into the Pentagon computer system. He thinks he is playing a wargame on that system, but reality mixes with the game and he brings the world to the brink of nuclear conflict. Modern day movies are populated with the most outrageous, savvy and lighting fast hackers. With a few clicks and keystrokes hackers can switch off systems, delete someone's entire digital identity, or blow up whole industrial complexes with nothing but some cleverly coded malware. Think James Bond, think Mission Impossible. While it will probably not surprise you that Hollywood is overdoing and overselling it, reality in cyberspace, while much less glamorous, is getting rather grim too. I will give you a few real life examples.

In 2009 and 2010 the Iranian nuclear facilities in Natanz were secretly sabotaged by means of a cyber operation we now know as Stuxnet.[1] The malware used caused the nuclear centrifuges to spin out of control while leaving the engineers at a loss for the reason why. This cyber-attack is generally attributed to The United States and Israel who were looking for a way to disrupt Iran's nuclear program, without using military means such as airstrikes. This cyber sabotage operation was most likely run by the CIA and the Mossad.

In 2015 the United States Office of Personnel Management, the chief human resources agency for the federal government, was hacked.[2] The files and personal details of millions of federal government employees with security clearances were stolen, making them vulnerable to blackmail and espionage. The so called OPM hack is attributed to China. It is a classic espionage case, but on an unprecedented scale, about which James Clapper, Director of National Intelligence reluctantly said: "You have to kind of salute the Chinese for what they did. If we had the opportunity to do that, I don't think we'd hesitate for a minute".[3]

The US presidential elections of 2016 were the target of so-called Russian influence operations aimed at disrupting the electoral process, and influencing the political debate and outcome of the election.[4] The tools were hack and leak operations – injecting damaging information for the democrats into the public debate – and online campaigns in which Russians impersonated American citizens and grass roots organisations. In this way the Russian military intelligence agency GRU subverted the holy grail of the democratic process: the election itself.

In 2017 Russian hackers launched destructive malware that is now known as 'NotPetya'.[5] The threat intel researcher that named it NotPetya, still apologizes for the lousy name for such a notorious virus. Although the malware masqueraded as a ransomware attack – in which case you have to pay to get your encrypted files back – in reality it destroyed every computer it infected and turned them into useless bricks. Though intended for Ukraine, NotPetya spread indiscriminately like wildfire and infected machines far beyond Ukraine. This was sabotage, or even cyber vandalism. The global damage was estimated at 10 billion US dollars and the operation was attributed to Russian military intelligence.

In late 2020 the story broke of the Solarwinds hack.[6] This was a crafty attack in which many companies and US government organisations were breached and compromised for – most likely- espionage purposes. The malware cleverly piggybacked on the security updates of the SolarWinds company that all these organisations paid for as a part of their digital security. The fact that the hackers used the digital supply chain for this hack was deeply disturbing to policymakers and the technical community. The hack was attributed to Russian intelligence. These are just a few of the more notorious cyber operations that have kept academics, threat intel researchers and policy

makers awake at night. They are all so called peace time operations, meaning they do not occur in times of war, nor rise to the level of armed conflict. However, some academicshave characterised our current digital times aptly as 'unpeace'[7], as it falls short of both peace and war. If we look at these quite diverse cyber operations a couple of first observations can be made:

- Firstly, all of these operations were allegedly conducted by intelligence agencies, but they do not necessarily correspond with what we consider to be classic espionage – in the sense of secretly gathering strategic information. This leads to questions about the role and function of intelligence agencies in cyberspace.
- Secondly, it brings to mind a classic question for those looking at the impact of technology on existing practices. Does the availability of new technology, or the technological changes in the operational context, make a difference for the activity itself? If espionage is the second oldest profession in the world, does the digitalisation of the work and the context of cyberspace make a difference? And if so, are we the talking about a quantitative or a qualitative shift?
- Thirdly, after all these operations the victimised state – but in some cases whole groups of states – clearly and publicly signalled that these were unacceptable cyber operations. They even signalled that they considered it be out of legal or normative bounds. But they never explicitly connect these operations to specific rules and legal principles that may have been breached. Also, in diplomatic negotiations at the UN about responsible state behaviour in cyberspace, intelligence agencies are never mentioned. This in spite of the fact that the operations that make diplomats worry about international security and stability in cyber space are often conducted by those agencies. They are the elephants in the room. They take up a lot of space but are not discussed.

Taken together these observations mean that it might be worth our while to talk about cyber intelligence and address the elephant in the room. To do so, there are many questions that we need to look into. What is intelligence and what is cyber intelligence? Where does it start and where does it end, and who gets to say so? Do interpretations of what cyber intelligence is and is not have repercussions for how we wish to govern – or not govern – the activities of intelligence agencies in cyberspace? What is their contribution to international security and/or insecurity? Why do international law and public state diplomacy by and large ignore the activities of intelligence agencies, and is that silence still useful in state to state relations in the digital age?

What is (cyber) intelligence?

For something that is often described as the second oldest profession in the world, espionage and intelligence are surprisingly undertheorized and underdefined. To a certain degree that is because the academic field is relatively young, predominantly historical, and is dominated by American and British scholars, many of them with ties to and/or tracks in intelligence itself. That does not disqualify them as academics but - as I always tell my students – it does colour their analysis and you need to be aware of that. Always look at *who* wrote the book or paper, perspectives matter.

What intelligence is, is often described by looking at what intelligence agencies *do*. Generally there is a core of activities that is relatively undisputed and more peripheral activities that are disputed. At the core is the so called intelligence cycle that has different stages: running from intelligence collection, processing, to analysis.[8] This is classic political espionage, focused on gathering strategic information and informing the political leadership of a country. The information gathering component is at the centre of all definitions of intelligence and the digital age obviously has a massive impact on this core function. But when we move away from the collection of information to more active and violent interference in the

affairs of other states - the James-Bond-licence-to-kill aspect if you like - the political and academic consensus on what is 'in' and what is 'out' starts to crack.

Some argue that "covert action, influence [operations], and counterintelligence should be considered as essential intelligence practices, even if they are missing from the canonical intelligence cycle".[9] Research on covert action tends to focus on four broad types of activities often presented according to their degree of the use of violence: (1) propaganda and information operations; (2) political action, such as funnelling money to a political party or fomenting riots; (3) economic covert action; and (4) paramilitary action, from training insurgent groups to assassination".[10] These activities directly interfere in the affairs of another state, are often violent, and try to undermine the social and political stability in that state. Many covert activities are subversive and secretly exploit political and social cleavages that are already present. Stirring up the fire of Brexit, Black Lives Matter or the deep divisions between Democrats and Republicans in the US is a sure way to increase social unrest and undermine social cohesion in society. It can be effective, but is also time consuming. In the words of Ron Deibert: "subversion is a "slow-burn" activity— it takes persistence, patience, and time".[11]

Covert action is disputed in the sense of whether it is considered to be part of intelligence, or not. Some see covert action as part and parcel of intelligence and some see covert action as 'the handmaiden of intelligence'.[12] In other words: separate, but connected. Others consider covert action to be something very different from intelligence, either because they consider it to be bad policy, or because they believe it is necessary but should be kept separately.[13] Given that most of these activities are conducted in secret it is perhaps not surprising that they are hard to classify – both empirically and politically. For Stout and Warner (former national security professionals turned academics) this is a reason to propose a tautological workaround. They simply argue that 'intelligence is as intelligence does'.[14] Whatever intelligence agencies *do*, sooner or later, becomes part of what intelligence agencies *are*.

Looking at the *purpose* of intelligence is another way to determine what intelligence is. The basic point of departure of most theories is that 'intelligence is a function of government'[15] or formulated slightly differently: intelligence is a third form of statecraft, next to war and diplomacy. In other words, intelligence is something states have in their toolbox to achieve strategic goals and avoid strategic mistakes. For example, by providing information that prevents tragic misinterpretations of the actions and intentions of others. That goes first and foremost for the information function: "Gathering information on an adversary that they wish to remain secret, using that knowledge to narrow the cone of uncertainty for decision makers, and doing so without being detected remain the cornerstones of intelligence."[16]

Covert action is usually seen as an instrument of foreign policy with the aim to influence events abroad more directly, while not being openly seen to do so. Some argue that the use of covert intervention can be a check on escalation of a conflict[17], but others see covert action and more generally grey zone operations as potentially escalatory, especially in the cyber domain where intentions are often especially hard to read.[18] American scholar Jon Lindsay, who considers the whole range of activities described above as 'in', sums it up by saying that 'intelligence is *secret* statecraft'.[19] Secrecy is perhaps the most defining characteristic of intelligence agencies and their activities. But in the digital age, secrecy is also becoming an increasingly problematic characteristic.[20] In the context of intelligence secrecy comes in two flavours: Secrecy can be either *covert*, which means that the identity of the actor is obscured, or *clandestine*, which means that the activity itself is obscured. These two forms often overlap, but not always. In the case of covert operations you can see what is happening and what the effects are, but you cannot see who has done it.

This gives governments 'plausible deniability' – a doctrine that allows senior officials to say that they 'neither confirm nor deny' responsibility for a certain covert action. Some states – especially those that are hard to name and shame because they are simply not ashamed, like Russia – even settle for implausible deniability: full throated and indignant denials of activities that everyone is pretty sure they have committed anyway.[21]

The digital age has not been kind to the vital role of secrecy for intelligence agencies. In pre-digital times intelligence agencies could be relatively sure that most of their activities would stay secret for a substantial amount of time. Most of their activities would only come out when the archives were de-classified and opened. In the current age of digital surveillance, open source intelligence, private contractors in intelligence, and data breaches of intelligence agencies themselves – think of Chelsea Manning and Edward Snowden– secrets are not that safe anymore. Peter Swire called this the 'declining half-life of secrets'.[22] Even more problematically, American intelligence agencies have allegedly even lost some of their most prized hacking tools. In 2017 it was claimed that hacking tools of the CIA – the so called vault 7 files[23] – and of the NSA – hacked by the ShadowBrokers[24] – were stolen and put out in the public domain. This is not only embarrassing, as these agencies managed to lose the crown jewels of their hacking tools, but also dangerous. Once out in the open, other actors – states and criminals – can use these hacking tools for their own gain, making everyone less cyber secure than before. In the digital age, secrecy is under pressure from multiple angles leading Aldrich and Moran even to suggest "that the very idea of 'secret intelligence' is beginning to look like a twentieth-century concept" that needs to be revisited. They maintain that we may be headed for a world in which 'there are no secrets, only *delayed disclosures*'.[25]

So things have changed in the digital age but academically 'the Cold War still looms over our present discussions'.[26] Much of the literature is historical research and is built on cold war scenarios and the context of the bi-polar order from before 1989. However, the Cold War-style 'rules of the game' were perhaps unique to that specific historic balance of power. During the cold war confrontations between intelligence agencies were often believed to avoid escalation of a cold war into a hot war.[27] And to a certain extent the rules were clear. There was some sense of agreed competition between 'the west' and 'the east' in this messy grey zone of espionage and covert action that allowed strategic competition between the superpowers without escalation. But those 'rules' allowed much more activities than just the gathering of strategic information that is the undisputed core of all definitions of intelligence. Subversion, information operations and covert action were all part of the cold war game. While it is not the most academic of sources, John Le Carré's characterization of cold war Berlin as a place where Eastern and Western intelligence agencies confronted each other on a daily basis is evocative and illustrative:

> In Berlin, the Firm [British intelligence] had agents of influence, agents of disruption, subversion, sabotage and disinformation. We even had one or two who supplied us with intelligence, though these were an underprivileged crowd, kept on more out of a traditional regard than any intrinsic professional worth[28]

However, some things have changed since the end of the cold war, both politically and technologically. Politically, in many western countries intelligence agencies have become more embedded in various forms of national oversight – not in the least because of scandals and abuses of powers.[29] Western intelligence agencies still have plenty of room to manoeuvre, but scrutiny of their activities has increased. Most western countries favour a balance approach between secrecy and transparency, typified by Amy Zegart as: "Too much secrecy invites abuse. Too much transparency makes intelligence ineffective".[30] However, transparency is not only up to governments themselves any more: hacks and leaks,

investigative journalists and academics[31], threat intelligence research and open source intelligence, such as the work of Bellingcat[32], all shed light on many of the activities that intelligence agencies would have preferred to have kept secret.

Cyber as a gamechanger?

The digital age has clearly changed the context, the playing field, as well as the activities of intelligence agencies themselves. Digital technology has brought change, but the question remains whether it has been a gamechanger. How are the, arguably not very well defined, activities of intelligence agencies affected by the digitisation of our existence. I propose there are at least four big changes: increase in scale, heightened ambiguity, massive expansion of the attack surface and trickle down insecurity, that require us to rethink how cyber intelligence agencies should operate.

The first thing that has changed drastically is the *scale* of operations that the digital world allows. That goes first and foremost for traditional espionage and intelligence gathering. We live in the age of mass surveillance and mass data gathering: the volume of data has exponentially grown and espionage has followed suit. No more taking pictures of documents after a midnight break in at the embassy, but hovering up information by the terabyte after computer systems have been breached. The hack of the Office for Personnel Management stood out not because of what the Chinese intelligence agencies were after, but because of the scale of the hack. Moreover, some believe that this hack was part of a larger set of operations and that the hacks of Anthem – an American health insurer – and United – an American airline – were part of the same effort. Together they give the Chinese a very granular insight into the lives of American government personal with a security clearance.[33] But also less traditional intelligence activities like sowing division through information operations and other subversive operations can be scaled up massively because of digital technology.[34] Deception and subversion used to be an elite affair in which leaders tried to trick each other and left the rest of us out of it. But today, 'cyber-enabled deception operations seek to trick us all, shaping mass opinions across borders'.[35] Moreover, 'the internet did not bring more precision to the art and science of disinformation'. According to Thomas Rid it made [it] 'harder to control, harder to steer, and harder to isolate engineered effects. Disinformation, as a result, became even more dangerous.'[36] Operations and effects that resemble covert actions are now also much larger in their scale and reach.[37] Sabotage operations like NotPetya operate at an unprecedented, almost global scale and travel at high speed.[38] As Warner argues 'cyberspace seems to have fixed covert action's problem of scale.[39]

The cyber dimension also introduces an *ambiguity* into intelligence operations that may produce unforeseen consequences. Roughly speaking most cyber operations look the same at the start of the operation. Any cyber operation starts with getting access to a computer network and then continues by moving through that network. It is only when the attackers start exporting information, undermine systems or put destructive malware in place that it becomes clear to defenders whether they are dealing with espionage, subversion or a destructive cyber-attack. For a long time it all looks the same. In the real world a tank rolling towards the border would not easily be mistaken for an espionage operation, but in cyberspace things are much more opaque. This ambiguity lies at the heart of what Ben Buchanan calls the cyber security dilemma: states will often assume the worst when their systems have been breached and may react accordingly.[40] The jury is still out on whether this ambiguity just feeds uncertainty or also fuels the risk of escalation– and to what extent – but the matter puzzles academics and policy makers.[41] Moreover, while ambiguity may be good for intelligence agencies when it comes to their own actions, those actions are not supposed to create *unforeseen* consequences. In cyberspace many classic distinctions blur[42] and one important distinction is that between cyber *military* operations and cyber *intelligence*

operations. While there are organisational and operational reasons *why* these blur at the edges, there have traditionally been very good reasons to keep them separate. Amy Zegart neatly sums up the problem: "The good news is that intelligence and warfighting are now much more connected. The bad news is that intelligence and warfighting are now much more connected".[43]

The digital age has also vastly expanded the *attack surface* for intelligence operations. To get access, to gather information, to disrupt and to sabotage is not just a matter of state organisations and actors anymore. The breaking and entering does not happen at the embassy building, but through flaws in the software of Microsoft, Google or Siemens. The Solarwinds operation even had its malware cleverly piggybacking on the security updates that the clients were diligently downloading to protect their networks. Destructive operations like NotPetya spread indiscriminately and wiped every computer its malware landed on. While many cyber intelligence operations are highly targeted, the net gets cast much wider than before and the damages spread wider too. Intelligence agencies find, steal and buy vulnerabilities in software to gain access to their targets.[44] But that is the software we as citizens and companies all depend on. Every software vulnerability that is deliberately left unpatched is an open door that may also be used by other state agencies or criminals. Some vulnerabilities are even deliberately and secretly planted in commercial soft- or hardware by intelligence agencies to make sure they will have privileged access through so called 'back doors' that only they know of.[45] But, as Bruce Schneier reminds us, there is no back door that only the good guys walk through.[46] Even with the limited visibility we have on cyber intelligence operations, we can safely say that they now involve all the digital products we use to live our lives, to an extent that was unimaginable in pre-digital times.

Lastly, the digital age has a *trickledown* effect when it comes to tools and capabilities. While high end cyber operations – whether they are espionage, sabotage or attacks – are usually the preserve of well-resourced state intelligence agencies, some tricks of the trade are copied easily. Once malware is found in the wild and analysed, it becomes available to others too and often it has quite a destructive life after being discovered.[47] Defending against known vulnerabilities is nowhere near as good as one would hope. Moreover, capabilities that were cutting edge five years back are much more commonplace today.[48] The American concept of Nobody but us (NOBUS)[49] – meaning that some malware and capabilities will be only in the hands of the United States as the top tier cyber power – is boastful to begin with and seems more like wishful thinking if we look at it in a wider timeframe. The dependence of cyber intelligence on tools, exploits and malware that are likely to spread to other state and criminal actors after they have been discovered, lost or leaked has security implications far beyond the contest between intelligence agencies.

Intelligence as the elephant in the cyber room

If intelligence operations are so ill defined and the cyber variants of intelligence operations cause politicians and the general public such worry and distress, one would expect policy makers and diplomats to discuss them as part of international relations and governance. However, cyber intelligence is still the elephant in the diplomatic room. Everyone knows it is there, but it does not get addressed. Espionage and intelligence have traditionally been part of international relations, but not by talking about it or by regulating it. Quite the contrary: silence seems to be golden when it comes to intelligence. By and large, foreign intelligence is not addressed by international law, but rather guided by a gentlemen's agreement between states that peacetime intelligence operations are allowed.[50] The fact that international law is silent on intelligence and espionage has been repeated so many times that it is practically a dogma.[51] This leaves 'don't get caught' as the prime informal rule and 'everybody does it' as the first line of defence when one does get caught.[52] This also means that the undefined character of intelligence – what is and what is not considered intelligence

– gets an extra layer of protection under this gentlemen's agreement. What is the need for strict definitions if we do not talk about it anyway. When pressed international law works around the issue by maintaining that 'the lawfulness of cyber espionage activities is no different from the lawfulness of other cyber operations: there is no general prohibition of cyber espionage, but the cyber operations used may breach specific norms of international law'.[53] In other words, intelligence activities may violate international law, but not *because* they are intelligence activities.

This silence on the issue of espionage and intelligence in international law, is often replicated in international diplomatic negotiations. In the UN negotiations on responsible state behaviour in cyberspace – the efforts of the Group of Governmental Experts (GGE) and the Open Ended Working Group (OEWG) – the delegates discuss at length how international law applies to the conduct of states in times of war and in times of peace. But espionage and intelligence are never mentioned in the GGE and OEWG consensus reports, and diplomats often explicitly exclude it from the conversation. We don't talk about intel.

This does not mean that states are happy about espionage and intelligence. Most, if not all, states have domestic legislation in place that criminalises espionage and intelligence activities if they take place in their countries. In other words: at the international level states turn a blind eye to what they consider to be criminal behaviour at the national level. By doing so states actively create and sustain the legal grey zone. Also, many of the public attributions that western states put out about cyber operations conducted against them, concern operations that are conducted by intelligence agencies or their proxies, varying from destruction and sabotage to more traditional espionage. Sometimes these formal government statements are then nuanced by their own intelligence agencies indicating that this is 'business as usual' as far as they are concerned.[54]

The fact that intelligence is not addressed at the international level in legal and normative terms is to a certain extent a result of international power politics. Although many states conduct espionage it is especially a favourite tool for the power politics of big states. Big states have always preferred to have some strategic ambiguity in international relations – as it gives them room to manoeuvre in the (legal) grey zone. Smaller states are generally better served by more legal and normative constraints on state behaviour. To some extent the international system still resembles the world of Thucydides in which the 'Strong do what they can and the weak suffer what they must'. The formal sovereign equality between states is in practice often cancelled out by power asymmetries.[55] Even though power inequalities have played an important part in state to state relations through the ages, the development of international law and norms for interstate behaviour – however imperfect and slow moving – has been a prominent feature of international life as well. Especially after World War II. Over time a body of international law has developed that puts limits on state behaviour in both times of war and peace. To state the obvious: international law in itself does not stop states from breaking the rules even when they have put their signature to it, nor does it fully negate power asymmetries. But it does lay down a framework that separates lawful from unlawful behaviour in times of conflict and that is the yardstick states use to call out other states when they violate those rules. You cannot bring war criminals to justice in a court – and that is extremely rare to begin with - if you have not defined what war crimes are.

While cyber intelligence is not war, I think there are ample reasons to revisit the idea that it is better left unaddressed. Ignoring the role of intelligence agencies in cyber conflict does not help to contain their activities. States will continue to push the boundaries of what is possible in cyberspace and by doing so they will extend and stretch the legal and normative grey zone. If other states do not contest and/or constrain such behaviour they will ultimately just codify that behaviour,

and it will become the norm.[56] Then cyber intelligence will indeed simply be what cyber intelligence does. While that may be good for some – especially the intelligence agencies of big states - it is not so good for smaller states, like the Netherlands, and it is not so good for the security of the digital world we all live and work in.

We need to talk about the elephant

If states continue along the road they have been traveling so far, then it will be state practice that shapes the norms in cyberspace. More specifically, it will be the state practice of the big states. Norms of what is appropriate will materialise from the behaviour of the intelligence agencies of states like Russia, the United States, North Korea and China to name a few of the most active and brazen actors in this space. Between those actors we have seen cyber operations varying from sabotage and digital vandalism, via information operations that stoke the fires of societal division, to espionage on an industrial scale. And all of these playing out on the digital infrastructure that we all rely on for our daily lives. As things now stand, smaller states are tacitly supporting this development by not challenging behaviour – or only in muted terms – because of the gentlemen's agreement that we do not talk about espionage and intelligence among states. By collectively propping up this dogma most states may well be acting against their own better interests. Their implicit support provides the cover for big states to develop practices that (a) most states will never use themselves and (b) are likely to damage their national and collective digital security.

So what would happen if states do decide to address the elephant in the room? Addressing a phenomenon that is so deeply steeped in secrecy and has been deliberately ignored in terms of international law and governance is never going to be easy, but neither is it impossible. The choice to explicitly not address espionage has been a political one, and nothing in politics is forever. I have no illusion about the speed of such processes though. Poznansky describes the history of the legal principle of non-intervention as a journey of hundreds of years, starting as 'an idea that international lawyers, philosophers and smaller states promoted but great powers mostly ignored' until it was finally codified in the United Nations Charter.[57] The digital age moves faster, but international law is notoriously hard to speed up.

If the grey zone in which intelligence agencies operate, gives the top tier cyber powers the room to manoeuvre and push the boundaries of what is considered acceptable behaviour, than for many states there is value in trying to *shrink* this grey zone. One logical place to start would be to determine what cyber intelligence practices are considered legitimate and what are considered illegitimate. That would require conceptual clarity and political courage.

States can try to shrink the grey zone by asking and answering questions like: Are there limits to intelligence activities in cyberspace as a result of scale, scope, targets, context, and the risk of unintended consequences? Some of the political reactions to mass surveillance suggest there are, but intelligence agencies themselves tend to err on the side of their own access to information and resist limits. Reckless and indiscriminate cyber operations like NotPetya could be discussed as an example of crossing the line when it comes to cyber sabotage operations.[58] Information operations, like hack and leak operations and disinformation campaigns, are a significant political problem in democratic countries, and could be part of some consensus on what should and should not be considered legitimate cyber intelligence operations.[59] Information operations are a thorny issue though: most of the activities qualified as foreign information operations are as yet not defined as "illegal" under national and international law making it harder to push back.

Discussing these questions – in spite of the dogma of not talking about intelligence - may pave the way to putting some limitations on the record in an effort to shape the normative field. Making norms explicit is a starting point to act on them

and to defend them. When it is in their national interest big states like the United States are sometimes prepared to make that cut. The Obama administration, when faced with industrial espionage on an industrial scale by China, very explicitly proclaimed a norm that separated political espionage, which they consider legitimate, from economic espionage, which they consider illegitimate.[60] So within the general rule that we do not address cyber intelligence, the US unilaterally carved out a new norm that serves its national interest and that it tries to police itself.[61] For smaller states there is strength in numbers. To some extent states are trying to shape the normative field at the national level where domestic legislation and oversight create boundaries for their own intelligence agencies. Lessons learned there might be pooled and uploaded into the international debate.[62] Other issues, like some of those identified above could be part of international discussions. Such debate is likely to start in smaller, likeminded groups before they will get any wider traction. It will be mini-lateralism, rather than global multilateralism, for the foreseeable future.[63]

As Thomas Hobbes wrote long ago: 'covenants, without the sword, are but words, and of no strength to secure a man at all'.[64] Normative frameworks that are not enforced provide little security, but failing to make norms explicit makes enforcing them harder and less legitimate. The absence of clarity does not do the case of cyber security any favours. There is work needed on both the clarity of the normative framework and on the political will and capacity to act on those norms.[65]

Global Security and Technology

For this inaugural lecture I chose to take you all down the rabbit hole of one specific subject, rather than sketching the broad outlines of the field of Global Security and Technology, which is the subject of my chair. That field has many rabbit holes that I - and my colleagues – will go down into in the coming years. For example: how will artificial intelligence impact on conflict and how will states balance their interest in using artificial intelligence for their own military advantage with their interest in governing such new technologies to ensure its globally responsible use?[66] Or: what is the impact of new European political concepts such as 'digital sovereignty' and 'strategic autonomy' on the ability of the EU to chart an independent course in a world of mounting geopolitical tensions?[67] Many of the questions that we study under the aegis of global security and technology are complicated governance issues involving national and international interests and actors, including states, companies and civil society. None of the questions that we study are well served by a single disciplinary approach. I firmly believe that to understand these global governance problems we need to talk across disciplines as well as keep the conversations between academia and policymakers going. Academics can offer new concepts and ideas, engage in debate, and share platforms with policy makers without losing track of either side's own role and responsibility. For both the connection between disciplines as the connection between policy and academia it is a blessing that I take up this chair at the Institute of Security and global Affairs. An institute that breathes multi- and interdisciplinarity and is located at the Leiden university Campus in the Hague, a city that is home to both national and international policy making.

Acknowledgements

'No man is an island, entire of itself' wrote John Donne[68] in 1624 and that is no less true for me now than it was in 2015 when I echoed his words in my inaugural lecture at Erasmus University Rotterdam. And again, I will name just a few of those to whom I owe a debt of gratitude.

I am grateful to the executive board of Leiden University, for the trust they placed in me by appointing me to the chair of Global Security and Technology. I am very grateful to Erwin Muller, the dean of the Faculty of Governance and Global Affairs, and Joachim Koops, scientific director of the Institute of Security and Global Affairs, for their support, and for making this appointment happen.

I am also grateful to the Task Force Cyber at the Dutch Ministry of Foreign Affairs for supporting our research and activities, but even more for the exchanges we have in figuring out the rules of the road in cyberspace.

It was Bibi van den Berg who pulled me into the institute with an offer I could not, and did not want to, refuse. I am happy I heeded Bibi's call to cyber. I thoroughly enjoy working at Institute of Security and Global Affairs. It houses many wonderful friends and colleagues that overlap with me and my interests in a jumble of Venn diagrams. The Cyber Security Governance group in particular is a wonderful, dynamic and ever growing group that I am fortunate and proud to be part of.

The cyber core team is the best and most fun team to work with. Many things happen, and usually at the same time, but we have fun getting it all together. Corianne, Monica, Arun, Lise and Lena: I look forward to keep working with you all in the coming years.

During my career I was fortunate to encounter mentors who helped me grow, usually by making room for me and entrusting me with responsibility. I am grateful for the guidance given to me along the way by Pauline Meurs, Godfried Engbersen, Wim van de Donk and Corien Prins.

I consider myself to be a rich man when it comes to friendship. I am happy and honoured by seeing so many of my older and newer friends in the audience here. Friendship is what makes life worth living.

My family is my foundation. Seeing them here together means more to me than I can express. Over the years we have become even tighter. I am very happy and proud that Wijnand and Lisette, our pater and mater familias, are here to celebrate with me.

On that foundation I built my own family. Linnet, you are my heart and I love traveling through life with you. We travel at high speed, but we travel together. And most importantly, we co-authored the greatest work we will ever do: our children Olivia and Julia.

Dear Olivia and Julia: hearing your names, must mean we are nearly done. You are the joy in my life and it is high time that we go and do something fun!

Ik heb gezegd!

Notes

1 For an overview and analysis of the Stuxnet attack see (for example): Kim Zetter (2014) *Countdown to Zero Day. Stuxnet and the Launch of the World's First Digital Weapon*. New York: Broadway Books; James Farwell & Rafal Rohozinski (2011) Stuxnet and the Future of Cyber War, *Survival*, 53:1, 23-40, DOI: 10.1080/00396338.2011.555586.

2 For an overview and analysis of the OPM hack see (for example): Joe Devanny, Ciaran Martin & Tim Stevens (2021) On the strategic consequences of digital espionage, *Journal of Cyber Policy*, 6:3, 429-450, DOI: 10.1080/23738871.2021.2000628; Dan Efrony and Yuval Shany (2018) 'A rule book on the shelf? Tallinn manual 2.0 on cyberoperations and subsequent state practice', *American Journal of International Law*, Vol. 112(4): 583–657.

3 Julianne Pepitone (2015) China Is 'Leading Suspect' in OPM Hacks, Says Intelligence Chief James Clapper', *NBC News*, June 25, 2015, https://www.nbcnews.com/tech/security/clapper-china-leading-suspect-opm-hack-n381881

4 For an overview and analysis of the US election interference campaign see (for example): Dan Efrony and Yuval Shany (2018); Florian Egloff (2020) "Contested Public Attributions of Cyber Incidents and the Role of Academia." *Contemporary Security Policy* 41 (1): 55–81. doi:10.1080/13523260.2019.1677324; Jens David Ohlin (2020) *Election Interference: International Law and the Future of Democracy.* Cambridge: Cambridge University Press

5 For an overview and analysis of NotPetya see (for example): Andy Greenberg (2019*) Sandworm. A New Era of Cyberwar and the Hunt for the Kremlin's Most Dangerous Hackers*. New York: Doubleday; Dennis Broeders, Els de Busser, Fabio Cristiano & Tatiana Tropina (2022) Revisiting past cyber operations in light of new cyber norms and interpretations of international law: inching towards lines in the sand?, *Journal of Cyber Policy*, 7:1, 97-135, DOI: 10.1080/23738871.2022.2041061

6 For an overview and analysis of the SolarWinds hack see (for example): Marcus Willett (2021) "Lessons of the SolarWinds Hack", *Survival*, 63:2, 7-26, DOI: 10.1080/00396338.2021.1906001; Devanny, Martin & Stevens (2021)

7 Lucas Kello (2017) *The Virtual Weapon and International Order*. New Haven: Yale University Press; see also Ben Buchanan (2020) *The Hacker and the State. Cyber Attacks and the New Normal of Geopolitics*. Cambridge (Mass.): Harvard University Press.

8 David Gioe, Michael Goodman and Tim Stevens (2020) Intelligence in the cyber era: Evolution or Revolution? *Political Science Quarterly* 135(2): 191-224, https://doi.org/10.1002/polq.13031, p. 209

9 Jon Lindsay (2021) Cyber conflict vs. Cyber Command: hidden dangers in the American military solution to a large-scale intelligence problem, *Intelligence and National Security*, 36:2, 260-278, DOI: 10.1080/02684527.2020.1840746, p. 262

10 Rory Cormac, Calder Walton and Damien van Puyvelde (2022) 'What constitutes successful covert action? Evaluating unacknowledged interventionism in foreign affairs', *Review of International Studies*, 48(1), 111-128. doi:10.1017/S0260210521000231, p. 112; Amy Zegart (2022) *Spies, Lies and Algorithms. The History and Future of American Intelligence*. Princeton: Princeton University Press, p. 172

11 Ronald Deibert (2022) "Subversion Inc: The Age of Private Espionage". *Journal of Democracy*, vol. 33, no. 2, pp. 28–44 (p. 32), see also: Lennart Maschmeyer; The Subversive Trilemma: Why Cyber Operations Fall Short of Expectations. *International Security* 2021; 46 (2): 51–90. doi: https://doi.org/10.1162/isec_a_00418, p. 54, 59; Thomas Rid (2020) *Active Measures. The Secret History of Disinformation and Political Warfare*. London: Profile Books.

12 Gioe, Goodman and Stevens (2020)
13 Mark Stout & Michael Warner (2018) Intelligence is as intelligence does, *Intelligence and National Security*, 33:4, 517-526, DOI: 10.1080/02684527.2018.1452593
14 Stout and Warner (2018)
15 Stephen Marrin (2018) Evaluating intelligence theories: current state of play, *Intelligence and National Security*, 33:4, 479-490, DOI: 10.1080/02684527.2018.1452567, p. 479.
16 Gioe, Goodman and Stevens (2020), p. 223
17 Austin Carson (2018) *Secret Wars. Covert Conflict in International Politics*. Princeton: Princeton University Press
18 Ben Buchanan (2016) *The Cybersecurity Dilemma. Hacking, Trust, and Fear between Nations*. London: Hurst & Company. See also: Jason Healy and Robert Jervis (2023) 'The Escalation inversion and Other Oddities of Situational Cyber Stability', pp. 21-59 in Robert Chesney, James Shires and Max Smeets (eds.) *Cyberspace and Instability*. Edinburgh: Edinburgh University Press.
19 Lindsay (2021), p. 262
20 Dennis Broeders (2016) 'The Secret in the Information Society', *Philosophy and Technology.* **29**, 293–305 https://doi.org/10.1007/s13347-016-0217-3
21 Rory Cormac and Richard Aldrich (2018) 'Grey is the new black: covert action and implausible deniability', *International Affairs*, Volume 94, Issue 3: 477–494, https://doi.org/10.1093/ia/iiy067; see also Keir Giles (2019) *Moscow Rules: What Drives Russia to Confront the West*, Washington, D.C.: Brookings Institution Press.
22 Peter Swire (2015). *The Declining Half-life of Secrets and the Future of Signals Intelligence. New America Cyber Security Fellows Paper Series no. 1, July 2015*. Washington: New America Foundation.
23 Patrick Radden Keefe (2022) The surreal case of a CIA hacker's revenge. *The New Yorker*. June 6 2022
24 Buchanan 2020: 240-267; see also Daniel Moore (2021) *Offensive Cyber Operations. Understanding intangible warfare.* Oxford: Oxford University Press, p. 83-84.
25 Quoting Mark Fallon in: Richard Aldrich and Christopher Moran (2019). 'Delayed Disclosure': National Security, Whistle-Blowers and the Nature of Secrecy. *Political Studies*, *67*(2), 291–306. https://doi.org/10.1177/0032321718764990, p. 294.
26 Joshua Rovner (2023) 'The Elements of an Intelligence Contest', pp. 17-42 in: Robert Chesney and Max Smeets (eds.) *Deter, Disrupt or Deceive. Assessing Cyber Conflict as an Intelligence Contest*. Washington DC: Georgetown University Press, p. 28
27 Steven Loleski (2023) 'The United States and Legitimizing Rules of the Game', pp. 134-150 in: Robert Chesney and Max Smeets (eds.) *Deter, Disrupt or Deceive. Assessing Cyber Conflict as an Intelligence Contest*. Washington DC: Georgetown University Press, p. 137
28 John Le Carré (2020/1986) *A perfect Spy*. London: Penguin Books, p. 612
29 Zachary Goldman and Samuel Rascoff (2016, eds.) *Global Intelligence Oversight. Governing Security in the Twenty-First Century.* Oxford: Oxford University Press; David Omand and Mark Phythian (2018) *Principled Spying: The Ethics of Secret Intelligence*. Oxford: Oxford University Press.
30 Zegart (2022), p. 7
31 Like the work of journalists like David Sanger, Kim Zetter and Ellen Nakashima, and the various journalist groups that worked on the Snowden files. In academia the work of Ron Deibert and his Citizen Lab at the University of Toronto stands out.
32 Eliot Higgins (2021) *We Are Bellingcat: An Intelligence Agency for the People*. London: Bloomsbury.
33 Ming Shin Chen (2019) 'China's Data Collection on US Citizens: Implications, Risks, and Solutions', *Journal of Science Policy & Governance*, Vol 15(1): 1-14.
34 Maschmeyer (2021); Michael Warner (2023) 'The Character of Strategic Cyberspace Competition and the Role of Ideology', pp. 43-59 in: Robert Chesney and

Max Smeets (eds.) *Deter, Disrupt or Deceive. Assessing Cyber Conflict as an Intelligence Contest*. Washington DC: Georgetown University Press; Richard Harknett & Max Smeets (2022) Cyber campaigns and strategic outcomes, *Journal of Strategic Studies*, 45:4, 534-567, DOI: 10.1080/01402390.2020.1732354

35 Zegart (2022), p. 266

36 Thomas Rid (2020) *Active Measures. The Secret History of Disinformation and Political Warfare*. London: Profile Books.

37 Lindsay (2021), p. 264

38 Monica Kaminska, Dennis Broeders, and Fabio Cristiano (2021) 'Limiting Viral Spread: Automated Cyber Operations and the Principles of Distinction and Discrimination in the Grey Zone.", pp. 59–72 in T. Jančárková, L.Lindström, G. Visky, and P. Zotz (eds.) *13th International Conference on Cyber Conflict: 'Going Viral'*. Tallinn: CCDCOE

39 Michael Warner (2023) 'The Character of Strategic Cyberspace Competition and the Role of Ideology', pp. 43-59 in: Robert Chesney and Max Smeets (eds.) *Deter, Disrupt or Deceive. Assessing Cyber Conflict as an Intelligence Contest*. Washington DC: Georgetown University Press, p. 49

40 Ben Buchanan (2016) *The Cybersecurity Dilemma. Hacking, Trust, and Fear between Nations*. London: Hurst & Company.

41 Carly Beckerman (2022) 'Is there a cyber security dilemma?', *Journal of Cybersecurity*, Volume 8, Issue 1, https://doi.org/10.1093/cybsec/tyac012; see for a related perspective based on uncertainty and risk management: Monica Kaminska (2021) 'Restraint under conditions of uncertainty: Why the United States tolerates cyberattacks', *Journal of Cybersecurity*, Vol 7(1), tyab008, https://doi.org/10.1093/cybsec/tyab008; for a perspective on the relationship between cyber-attacks, escalation and secrecy versus public attribution, see: Gil Baram (2023) 'A sliding scale of secrecy: toward a better understanding of the role of publicity in offensive cyber operations', *Journal of Cyber Policy*, DOI: 10.1080/23738871.2023.2184708

42 Lene Hansen and Helen Nissenbaum (2009) Digital Disaster, Cyber Security, and the Copenhagen School, *International Studies Quarterly*, Volume 53, Issue 4: 1155–1175, https://doi.org/10.1111/j.1468-2478.2009.00572.x

43 Zegart (2022), p. 193.

44 See Nicole Perlroth (2021) *This is how they tell me the world ends. The Cyber Weapons Arms Race*. London: Bloomsbury; Lillian Ablon, Martin Libicki and Andrea Golay (2014) *Markets for Cybercrime Tools and Stolen Data*. Hackers' Bazaar. Santa Monica: Rand Corporation.

45 Susan Landau (2014) 'Making Sense of Snowden, Part II: What's Significant in the NSA Revelations', *IEEE Security & Privacy*, 12 (1): 62–64.

46 Bruce Schneier (2014) *iPhone Encryption and the Return of the Crypto Wars*. Schneier on Security (6 October 2014): https://www.schneier.com/blog/ archives/2014/10/ iphone_encrypti_1.html.

47 Lillian Ablon and Andy Bogart (2017) *Zero days, thousands of nights: The life and times of zero-day vulnerabilities and their exploits*. Santa Monica: Rand Corporation

48 Dennis Broeders (2015) *The Public Core of the Internet. An international Agenda for Internet Governance*. Amsterdam: Amsterdam University Press.

49 Nicole Perlroth (2021), p. 136-138; Buchanan (2020), p. 47.

50 Sergei Boeke and Dennis Broeders (2018) 'The Demilitarisation of Cyber Conflict', *Survival* 60 (6):73–90. doi:10.1080/00396338.2018.1542804, p. 77; Gary Brown and Andrew Metcalf (2014) 'Easier Said than Done: Legal Reviews of Cyber Weapons', *Journal of National Security Law & Policy*, vol. 7: 115–38; Michael Schmitt (2017, ed.) *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*. Cambridge: Cambridge University Press, p. 168-173.

51 Asaf Lubin (2020) 'The Liberty to Spy', *Harvard International Law Journal*, 61 (1): 185–243.

52 Boeke and Broeders (2018), p. 77

53 François Delerue (2020) *Cyber Operations and International Law*. Cambridge: Cambridge University Press, p. 200

54 Joe Devanny, Ciaran Martin & Tim Stevens (2021)

55 Stephen Krasner (1999) *Sovereignty. Organized Hypocrisy*. Princeton: Princeton University Press

56 Ilina Georgieva (2020) The unexpected norm-setters: Intelligence agencies in cyberspace, *Contemporary Security Policy*, 41:1, 33-54, DOI: 10.1080/13523260.2019.1677389

57 Michael Poznansky (2020) *In the Shadow of International Law. Secrecy and Regime Change in the Postwar World*. Oxford: Oxford University Press, p. 18

58 Kaminska, Broeders and Cristiano (2021).

59 See for example: Ido Kilovaty (2018) "Doxfare: Politically Motivated Leaks and the Future of the Norm on Non-Intervention in the Era of Weaponised Information." *Harvard National Security Journal* 9: 146–179; Jens David Ohlin (2020) *Election Interference: International Law and the Future of Democracy.* Cambridge: Cambridge University Press; Dennis Broeders (2021) "The (Im) possibilities of Addressing Election Interference and the Public Core of the Internet in the UN GGE and OEWG: a Mid-Process Assessment." *Journal of Cyber Policy* 6 (3): 277–297. doi:10.1080/23738871.2021.1916976.

60 Martin Libicki (2017) "The Coming of Cyber Espionage Norms", pp. 7-23 in H. Rõigas, R. Jakschis, L. Lindström, and T. Minárik (eds.) Defending the Core, Tallinn: NATO CCD COE Publications

61 However, the initial US- Chinese 'agreement' to not conduct economic espionage is generally considered not to have held very long. See for example Nigel Inkster (2020) *The Great Decoupling. China, America and the Struggle for Technological Supremacy*. London: Hurst Publishers.

62 Dennis Broeders, Sergei Boeke and Ilina Georgieva (2019) *Foreign intelligence in the digital age. Navigating a state of 'unpeace'*. The Hague Program For Cyber Norms Policy Brief. September 2019; Zachary Goldman and Samuel Rascoff (2016) *Global Intelligence Oversight. Governing Security in the Twenty-First Century.* Oxford: Oxford University Press; see also the project 'European Intelligence Oversight Network (EION)' run by the Berlin thinktank Stiftung Neue Verantwortung (https://www.stiftung-nv.de/en/eion)

63 Chris Brummer (2014) *Minilateralism. How Trade Alliances, Soft Law and Financial Engineering are Redefining Economic Statecraft.* Cambridge: Cambridge University Press

64 Thomas Hobbes (1848/1894) *Leviathan: Or, The Matter, Form, and Power of a Commonwealth Ecclesiastical and Civil*. London: Routledge and Sons, Part II – of Commonwealth, chapter XVII.

65 Dennis Broeders, Els de Busser, Fabio Cristiano & Tatiana Tropina (2022).

66 Fabio Cristiano, Dennis Broeders, Francois Delerue, Frederick Douzet and Aude Géry (2023, eds) *Artificial Intelligence and International Conflict in Cyberspace.* Abingdon: Routledge.

67 Broeders, D. (2022, ed.) Digital Sovereignty: From Narrative To Policy?, EU Cyber Direct, https://eucyberdirect.eu/research/digital-sovereignty-narrative-policy; Dennis Broeders, Fabio Cristiano, Monica Kaminska (2023) "In Search of Digital Sovereignty and Strategic Autonomy: Normative Power Europe to the Test of Its Geopolitical Ambitions", *Journal of Common Market Studies*, online first, https://doi.org/10.1111/jcms.13462

68 John Donne (1624) *Meditation XXVII*

Prof. dr. Dennis Broeders

Dennis Broeders is professor of Global Security and Technology at the Institute of Security and Global Affairs, Faculty of Governance and Global Affairs of Leiden University. His research and teaching broadly focuses on the interaction between international security, technology and policy, with a specific interest in international cyber security governance.

He is the PI and senior fellow of *The Hague Program on International Cyber Security* (2022-2025) and co-PI and project coordinator of the *EU Cyber Direct - EU Cyber Diplomacy Initiative* (2021-2024). Previously he was the senior fellow of *The Hague Program for Cyber Norms* (2018-2020). He served as a member of the Dutch delegation to the UN Group of Governmental Experts on international information security and the Open Ended Working Group (2019-2021) as an academic advisor.

Before joining Leiden university he was a senior research fellow and project coordinator at the Netherlands' Scientific Council for Government Policy in the Hague and professor by special appointment of Technology and Society at Erasmus University Rotterdam.

Universiteit Leiden