Foreign intelligence in the digital age. Navigating a state of ‘unpeace’.

Broeders D.W.J., Boeke S., Georgieva I.

2019 Policy brief

Foreign intelligence in the digital age

Navigating a state of 'unpeace'

Dennis Broeders, Sergei Boeke and Ilina Georgieva

THE HAGUE PROGRAM for Cyber Norms

Universiteit Leiden

Suggested citation:
Broeders, D., S. Boeke and I. Georgieva. (2019).
Foreign intelligence in the digital age. Navigating a state of 'unpeace'.
The Hague Program For Cyber Norms Policy Brief. September 2019.

Foreign intelligence in the digital age: navigating a state of 'unpeace'

Introduction

This policy brief covers the behaviour of intelligence agencies in cyberspace and possible normative constraints on that behaviour. Most known cyber operations by intelligence agencies are so called 'below-the-threshold' operations, and some stretch beyond what is commonly understood to be 'foreign intelligence gathering' to include covert action and influence campaigns. The digital domain facilitates new possibilities for classic intelligence tasks, but also entails new risks and (un)intended consequences such as threats to civilian use of the internet and grey zones of accountability. Importantly, the operations of intelligence services in cyberspace can have a negative impact on international peace and stability. In terms of regulation, intelligence agencies are the proverbial elephants in the room when states discuss the applicability of International Humanitarian Law (IHL) to the online world. The military-dominated legal framework does not fit well with actual state practice in cyberspace.[1] States are reluctant to discuss the specific operations of their intelligence agencies. This trend is unlikely to halt.

In order to explore the role of foreign intelligence agencies in cyberspace and the (im)possibilities of oversight and regulation thereof, *The Hague Program for Cyber Norms* convened 15 experts in a workshop in The Hague in April 2019. The experts were all from Europe and North America and about half of the participants were (former) members of foreign intelligence agencies, both civilian and military. The other participants were academic experts and members of intelligence oversight bodies. The workshop was held under the Chatham House rule.

Foreign intelligence in the digital age: blurred boundaries and practical challenges

The question of regulating foreign intelligence agencies and their practices has surfaced as a result of major transformations in how intelligence works in the digital age. Internally, technological advancement and the pervasiveness of information and communication technology (ICT) have blurred the contours of traditional intelligence modus operandi. Digitization has vastly increased the scope of passive foreign intelligence gathering and paved the way for new and more aggressive cyber operations, that do not necessarily fit with the classic paradigm. Foreign intelligence agencies are – allegedly – responsible for some of the most notorious cyber operations known to date. Recent operations like WannaCry and especially NotPetya are often considered 'game changers' – because of the indiscriminate damage done – leading to calls for regulation of cyber

1. Sergei Boeke & Dennis Broeders. (2018). "The Demilitarisation of Cyber Conflict", *Survival,* 60(6), pp. 73-90.

operations. Externally, the exposure of many cyber intelligence operations (followed by recent trends of public attribution) have lured intelligence agencies out of the traditional shadows in two unprecedented ways. First, by triggering legislative reforms in a number of countries and secondly, by forcing agencies to be more visible and diplomatic in its relation with the wider public. However, even with the increasing number of cases in the public domain, the experts in the workshop were unanimous in their insistence that this was merely the 'tip of the iceberg'.

The blurred intelligence landscape brings about numerous practical and conceptual questions. For one, it remains unclear whether and how existing intelligence categorizations apply to cyber operations conducted by foreign intelligence agencies. As these categorizations are shifting, the question of how these operations relate to the international legal order becomes a concern. This question is hampered by international law's (IL) limited relationship with intelligence practices – which by and large does not address foreign intelligence – but becomes increasingly unavoidable because many of the exposed cyber operations set alarming precedents. This was evidenced by a categorization exercise conducted among the experts of the workshop. Participants in the exercise were asked to allocate cyber operations with different levels of intensity to various activities (reconnaissance, espionage, bulk collection, influence, sabotage) that intelligence agencies might conduct in peacetime. Furthermore they reflected on how key intelligence concepts relate to practice and whether the examined conduct can be considered foreign intelligence 'fair game' or should be considered contested. The experts were further invited to reflect on the normative implications of the examined conduct.

Table 1: Categorisation of scope and legitimacy of cyber operations

Legend

- Anthem
- Belgacom hack
- BGP hijacking
- Bull Run
- DDos attacks on US banks
- Nitro-Zeus
- NotPetya
- OPM hack
- PRISM
- Russian hack of Ukrainian energy grid
- Russian info ops US elections 2016
- Saudi-Aramco
- SONY hack
- Stuxnet
- WannaCry

The participants considered the intent, target, legal authority and oversight when placing operations in categories. This then led to the determination of whether the operations were considered to be 'fair game' or not (see table 1). Political espionage and bulk collection were seen as the least problematic cases to place under the foreign intelligence umbrella. However, the end-use of the collected data, as well as particular features of the authorizing national legislation could still potentially affect the operation's legitimacy and thus categorization. Many of the discussed operations were labelled as 'sabotage' and categorized as 'contested' rather than 'fair game' for foreign intelligence agencies. This was largely because they posed a serious challenge to stability in cyberspace and the risk of escalation was considered high. Some experts commented on the need to forbid sabotage under the auspices of foreign intelligence actors altogether. However, though aware of the difficulty of reconciling sabotage activities with traditional foreign intelligence responsibilities (and corresponding statutes), practitioners recognized that some intelligence services do conduct them in cyberspace. Internal and external narratives about foreign intelligence operations may then diverge widely, contributing to the creation of strategic operational ambiguity. This has contributed, amongst others, to the view among the experts that foreign cyber operations are by and large designed to operate beyond the boundaries of International Law.

Strategic incentives, benefits and calculus

If so many of the revealed cyber operations are simultaneously considered 'contested' as well as regular practice among some agencies, then what is the calculus behind doing these operations? Traditionally, intelligence gathering is considered to be legitimate state activity. This, however, raises questions of proportionality due to the reach that the digital domain facilitates and the potential scale of effects. Cyber operations that have the character of influence operations or sabotage are more contested. Moreover, it is not a level playing field: intelligence agencies differ widely in their legal room to manoeuvre and the oversight of their activities. For some states cyber operations are an exercise of power that provides value for money. It allows them to operate below the threshold of armed conflict, creating a permanent state of 'unpeace'; a permanent tension in which some countries thrive.[2] More generally, the fact that some foreign intelligence cyber operations blur into what could be considered part of the portfolio of military and/or security agencies reflects the exploratory nature of the current cyber intelligence environment. In order to formally keep operations below the threshold, it has become common practice to disguise military 'preparations of the battlefield' as foreign intelligence activities. Lack of international laws and norms specifically aimed at foreign intelligence, new opportunities provided by technology and uncertainty about the behaviour of adversaries (and allies) in this space means that states and their foreign intelligence agencies want to keep their options open and their cards close to their chest. However, the debate about cyber operations has become more public in recent years. This is due to the exposure of cyber operations, the indiscriminate and damaging nature of some operations and the fact it is increasingly difficult to keep secrets.[3] It also signals discontent with at least part of the status quo.

2. Lucas Kello. (2017). *The Virtual Weapon and International Order.* New Haven and London: Yale University Press.
3. 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.

Attribution

One example is the increase of public attribution of cyber operations, often involving intelligence agencies exposing the operations of adversarial intelligence agencies. If 'attribution is what states make of it', [4] then so far it has been mostly western states trying to figure out the strategic value of public attribution of cyber operations.[5] Calling out the cyber operations of adversarial states has been predominantly a 'western affair'. China and Russia, for example, have not made any *formal* attributions, although they frequently accuse the West of digital espionage and breaching their systems. The role of intelligence agencies in attribution is complex. Intelligence agencies will always provide (unsolicited) information to their government about adversarial intelligence and cyber operations. It is up to the government to decide whether they want to use this information for a public attribution. As a rule, intelligence agencies are reluctant to disclose information on their sources. This applies equally to cyberspace, and information on adversarial operations could result in the loss of implants or access to networks. Sometimes, the protection of intelligence sources and methods is partially facilitated by private companies' research on the origin of cyber operations. Private security companies, as well as the targets themselves, can create the initial space for the respective attribution campaign. Some 'Advanced Persistent Threats' were originally 'outed' by private cyber security companies and in the case of the Sony hack, the company itself made the hack public. Any formal state-led public attribution will, at a minimum, disclose the detection of the act and its perpetrator. At most it can disclose forensic evidence, probably provided by intelligence agencies and/or law enforcement agencies.

So far, many of the political attributions have been relatively light in terms of evidence. This differs from the attributions under (national) criminal law, mostly the FBI indictments, that contain much more detail. The recent 'trend' of joint attributions and 'attribution coalitions' may raise the bar on the point of evidence though. As intelligence agencies are often an important source of information this puts them on the spot. What level of evidence is required to point the finger? At an individual? At a state? And what level of evidence is required to convince allies to sign up to attribution or an attribution coalition? A degree of trust is necessary, but to accuse a state, allies will need more. What do they need to see in order to be convinced, and what do they feel should be made public in order to substantiate the accusation? How can attribution coalitions deal with the fact that some states are part of close circles of confidence (5 eyes, 9 eyes) and others are outside? Again, states and their intelligence agencies will have to balance compromising or even burning sources with the political desire to collectively attribute. A mitigating factor for this would be the confidence intelligence agencies have that they can replace the lost access and sources by other means. This would make the calculus for the top tier cyber intelligence states easier, as they would suffer more limited losses of (re)sources. This contributes to attribution as a new privileged domain of the top tier cyber and intelligence states, perhaps shared with some of the international top tier cyber security companies.

4. Thomas Rid & Ben Buchanan. (2015). "Attributing Cyber Attacks", *Journal of Strategic Studies,* 38(1-2), pp. 4-37.
5. Dan Efrony & Yuval Shany. (2018). "A Rule Book on the Shelf? Tallinn Manual 2.0 on Cyber Operations and Subsequent State Practice". *American Journal of International Law,* 112(4), pp. 583-657.

The debate about attribution has become bound up with the debate about consequences. If attribution is to signal that a law or a norm has been broken, then what message does it send if there are no consequences? Some experts voiced concerns about potential unintended consequences of such campaigns, especially regarding the gap between initial expectations and final outcome of the cyber attribution. For that reason, some countries do not attribute or join attribution coalitions, if they know that diplomatic relations will stand in the way of actually imposing consequences. Moreover, the cases in which consequences were imposed have usually not exceeded the level of 'retorsion', which is allowed to states under international law and does not have any evidentiary requirements.[6] Both the US and the EU – the latter through the newly established EU cyber sanctions regime[7] – are increasingly going down the route of sanctions. It is important to realize that even though attribution is in essence political, sanctions can be legally challenged and should be based on solid evidence, especially if they rise above the level of retorsion.[8] The demand for attribution and consequences is likely to grow. Attribution will be on a case-by-case basis but different modes of attributing are likely to emerge on each side of the Atlantic. The US will want to avoid becoming predictable and follow a logic of 'strategic ambiguity', whereas the EU has laid down a framework for cyber sanctions that creates at least some degree of predictability. However, the EU cyber sanctions regime also opens attribution up to being legally challenged in the European Court of Justice by those individuals and legal persons that have been placed on the sanctions list.

Information operations

Traditionally, states like China and Russia are concerned with information security, whereas western countries focus on cyber security. Although the role of information operations in (military) conflict has ancient roots, misinformation, disinformation and influence operations have only taken centre stage since the 2016 US presidential elections. Whereas Russian and Chinese military and cyber doctrine have long underlined the importance of influence operations, American cyber doctrine's reference to the "integration of cyberspace operations with information operations" is only recent.[9] The integrity of information in the public digital domain appears to be a new battlefield and foreign intelligence agencies may be involved in it, both in offense and in defence.

Disinformation is elusive in nature. Its purpose is to slow down or complicate decision-making and destabilise domestic politics by influencing public and political opinion. Also, by inflating some (fake) news, other topics can be crowded out of the debate: if we spend all our time talking about American elections and collusion, we are not discussing Crimea and Donetsk. Also, influence operations do not necessarily break domestic laws. There are victims, but there is very little crime. Disinformation becomes even more elusive when true and false information are blended, further diluting the 'crime'. Disinformation also requires fertile political ground in the target state

6. See the upcoming policy brief on *Attribution and Evidence* by The Hague Program for Cyber Norms and EU ISS's EU Cyber Direct project.
7. Council of the European Union. (2019). "Council decision concerning restrictive measures against cyber-attacks threatening the Union or its Member States", 7299/19, 14 May 2019.
8. See for example, Karine Bannelier and Theodore Christakis. (2017). "Cyber-Attacks. Prevention-Reactions: The Role of States and Private Actors", *Les Cahiers de la Revue Défense Nationale,* Paris. Chapter 2.
9. US Cyber Command. (2018). *Achieve and Maintain Cyberspace Superiority.* Command Vision for US Cyber Command, p. 9.

to actually work. Even the best information operations cannot create political instability out of thin air. This makes it harder to defend against. The most durable defence would be to address the fertile ground of discontent and political gullibility (and even conspiracy mindedness) of the general population, aiming at macro level solutions through education and citizenship building. Calling out the narrative of disinformation and attributing it to adversarial states may require a role for intelligence agencies. But, as with attribution, this would place them in a role as 'arbiter of truth'. Even though the essential role of intelligence agencies is to speak truth to power – i.e. relating 'the truth' to their own government – their methods of obtaining information are often clandestine and involve deception. The wider (international) public generally does not equate intelligence agencies with truthfulness. A dark reading of recent changes in American military cyber doctrine, which introduced 'defending forward' and 'persistent engagement' as new key concepts,[10] combined with the ambition to 'integrate cyberspace operations with information operations' mentioned above, suggests that the US may be gearing up to 'fight fire with fire', with the integrity of information in the public domain as the main target and victim. Other major cyber powers may follow suit.

The structural dilemma underlying the role of intelligence agencies in cyberspace is that no state appears ready to relinquish capabilities at this point in time. However, the strategic advantage of cyber capacities for top tier states is grounded in both superior capabilities and asymmetry of capabilities. This calculus may change as the number of capable actors increase. Given that the learning curve for cyber can be steep and certain capabilities are relatively easy to acquire or purchase, this is not a fictional scenario for a determined actor. This suggests that one way forward is to start discussing taking certain activities or operations off the table. Vulnerability Equities Processes hint in that direction, as do calls to protect global supply chain integrity. Also, calls to protect 'the public core of the internet' and norms against intentionally weakening encryption and standards such as WiFi and SSL follow a logic of not poisoning the well we all drink from. Even though this logic does not break the fundamental dilemma, it may be the best starting point still.

Essential elements of accountability

National law and oversight mechanisms can function as confidence building measures (CBMs). Just as intelligence agencies can be considered norm entrepreneurs through their actual behaviour, so too should the bodies that regulate their operations.[11] After the Snowden leaks in 2013, many western states started to reform the laws and institutions that ensured oversight and accountability for national security agencies and foreign intelligence agencies.[12] At the same time these new legal frameworks often codified the extra-legal practices of intelligence agencies that were exposed. To many critics one of the main effects of these exercises was a legal "white washing" or formalisation of standing practices, rather than a curtailment of those practices.

10. Nina Kollars & Jacquelyn Schneider. (2018). "Defending Forward: The 2018 Cyber Strategy is Here", *War on the Rocks,* 20 September 2018.
11. Ilina Georgieva. (forthcoming). 'The Power of Norms Meets Normative Power', in: Dennis Broeders and Bibi van den Berg (eds.), *Governing Cyberspace: Behaviour, Power and Diplomacy,* 2020, Rowman & Littlefield.
12. David Omand & Mark Phythian. (2018). *Principled Spying: The Ethics of Secret Intelligence.* Oxford: Oxford University Press.

In many countries, previously existing regulatory frameworks consisted of patchworks of dated laws that were only accessible to the initiated. Several countries have replaced these by new and coherent frameworks. Modus operandi that were intrusive or controversial (or both), were analysed and debated. Where there was an operational case for their use, restrictive criteria were imposed on their deployment. This has increased national legitimacy, although the legislative processes in countries like the UK and the Netherlands also revealed deep divisions on the issue. The transparency of these new laws may also have an international effect. On the one hand, through legislating more clearly what and how foreign intelligence agencies are permitted to operate, states signal to others what principles lead and shape activities. Second, transparency provides other states assurances of intentions and capabilities, decreasing mistrust and the risk of misunderstandings and escalation.

There are several actors that influence oversight and accountability. First, for their member countries, jurisprudence of the European Court of Justice (ECJ) and the European Court of Human Rights (ECHR) have influenced national laws on data sharing and surveillance practices. For example, the UK's investigatory Powers Act 2016 was drafted with European law in mind, although this did not prevent the UK High Court from ruling in April 2018 that it violated EU law and needed to be amended.[13] The criteria of necessity and proportionality for measures that infringe on citizens privacy have thus been codified in member states' national laws. Other actors that have contributed to constraining intelligence services are technology companies such as Microsoft, Google and Facebook. They have encrypted their customers' data, launched initiatives for global norms for state behaviour (Microsoft) and publicized the number of government requests for data that they have received from law enforcement (also concerning counterterrorism). The first has complicated interception for intelligence agencies, the second involves a topic that used to be the exclusive remit of states, and the third involves court orders that were historically considered as secret or confidential. Western intelligence agencies now publically support the idea that oversight and public trust are vital to their operations. GCHQ director Jeremy Fleming stated in 2019 that "[we] must have the legal, ethical and regulatory regimes to foster public trust, without which we just don't have a licence to operate in cyberspace".[14] However, intelligence agencies have always operated at the edges of their license, and this is unlikely to change, especially in the rather murky terrain of cyber space.

Another important constraining factor on intelligence agencies is their peers. Intelligence sharing is considered essential to combat transnational threats like international terrorism, and many forms of international cooperation have developed in the past years. In the Five Eyes alliance, the intelligence communities of the US, the UK, Canada, Australia and New Zealand, cooperate in a structured and unrivalled fashion. Their services share platforms & systems, working practices and exchange personnel. The alliance works because of a shared language and culture, and similar institutional landscapes, especially in the way their intelligence services are structured and politically embedded. This has led to a convergence of their intelligence communities, resulting in a certain homogenization of intelligence practices. This equally applies to accountability and

13. Ian Cobain. (2018). "UK has six months to rewrite snooper's charter, high court rules", *The Guardian,* 27 April 2018.

14. Jeremy Fleming. (2019). "Director GCHQ's Speech at CYBERUK 2019", 24 April 2019.

oversight procedures. This isomorphic convergence can mean that where oversight is effective, best practices will spread across the board. Where ineffective, it can lead to a race to the bottom.[15] In other countries oversight and accountability structures vary enormously, and many different constructs (ex ante, ex post or combinations thereof) have been devised. The Dutch intelligence community, now required to weigh the benefits versus the risks of partnerships with other intelligence services, has already had to ask its peer services how they treat personal data to be able to make the case for a working relationship.

Intelligence oversight can only be effective if several criteria are met. First, oversight bodies must be completely independent, well-resourced and sufficiently staffed to be able to review the work of the intelligence services. These, in turn, will also need extra staff to meet the additional regulatory requirements, and some have complained that the administrative burden has increased, detracting from operational capacity. A response from oversight would be that this should only lead to a greater financial claim on the budget, and not a decrease in safeguards and protections. Secondly, oversight bodies must have complete freedom to investigate and report, preferably in the open and to parliament, and must therefore have unconditional and unlimited access to intelligence agencies and their information (with the exception of source names). If intelligence agencies determine what and when can be viewed by oversight, the role of the latter will be much diminished. Third, the criteria for weighing which special measures (such as bulk hacks) can be used under which circumstances need to be clear. For some services these criteria are just proportionality and necessity; others have included subsidiarity. While foreign citizens should intrinsically have the same right to privacy as national citizens, it is understandable that the procedures differ when warrants/permissions are requested. However, the international nature of internet traffic does not make the distinction easier. Finally, besides the necessity of oversight on cyber network exploitation and cyber network attack, it should be self-evident that covert operations, where information is used to manipulate a target audience, should also be subject to oversight and the criteria of necessity and proportionality.

However, oversight will not be able to address the structural dilemma that no state is willing to relinquish offensive cyber capabilities at this point in time. This plays out especially with intelligence agencies as they, rather than the military, conduct most cyber operations. Uncertainty about adversarial state behaviour and intentions pushes some intelligence agencies towards cyber operations that are considered 'contested' by their own admission. In the military domain restraining state behaviour has followed two main models: the Hague and the Geneva conventions. Under the regime of The Hague conventions (1899 and 1907) states declared certain weapons as out of bounds for use in conflict. Even though elements of the initial conventions were violated by some parties during the first and second world war, a strong international regulatory regime did evolve on what is permissible in war and what is not (ius in bello). Moreover, their spirit lives on in many treaties regulating weapon bans (landmines, chemical weapons) and non-proliferation regimes.

15. Richard Morgan. (2016). "Oversight through Five Eyes: Institutional Convergence and the Structure of Oversight of Intelligence Activities", p. 38 in: Zachary K. Goldman and Samuel J. Rascoff (eds.). (2016). *Global Intelligence Oversight: Governing Security in the Twenty-First Century.* New York, NY: Oxford University Press, USA.

The Geneva conventions had a different focus: who and what cannot be targeted under which conditions. Protecting the civilian population and taking certain organizations and objects off the list of legitimate targets for military actors[16] provides a different way of trying to get states to restrain themselves. Given the profound disagreement about whether it is feasible and productive to talk about cyber weapons in the military domain – let alone in the domain of cyber intelligence – the Hague rationale does not seem a productive way forward at this point in time.[17] The logic of the Geneva convention is already present in some of the international thinking on regulating responsible state behaviour in cyberspace. For example, the norms of not attacking critical infrastructure or CERTs in the 2015 UNGGE consensus report[18] follow the Geneva logic of taking things off the table. Other proposals, such as those of the protection of the public core[19] of the internet, build on the same logic, extending it to the core infrastructure of the internet itself.

In conclusion, the domain of intelligence oversight – until recently a rather marginal and national affair – should be given more weight. This can be done both in a horizontal and vertical fashion. A good horizontal initiative is the *Joint Statement Strengthening International Oversight Cooperation* in 2018 by the intelligence oversight committees of Belgium, Denmark, the Netherlands, Norway and Switzerland.[20] While the intelligence services of these countries share the same values, they have different mandates, rendering parallel or shared investigations between the oversight committees impossible. Nonetheless, international cooperation can push the level of unnecessary secrecy down, work on shared approaches and contribute to the debate on how to apply rules in cyberspace. Moreover, as a general principle the 'overseers' should be able to follow those they oversee. If the work of intelligence agencies becomes more cooperative and transnational, oversight should be able to follow suit. From a vertical perspective, exposure of oversight and accountability initiatives in high-level international fora, such as the UNGGE, would potentially not only serve as a confidence building measure, but could also directly contribute to establishing rules of the road for state behaviour in cyberspace.

Conclusion

Intelligence agencies are the main actors in the current state of digital 'unpeace' that is characterised by low-level cyber conflicts and tensions. The growth of activities – sometimes arguably beyond what is commonly considered foreign intelligence collection – has been accompanied by both new or additional legislation attempting to ground foreign intelligence agencies in the rule of law. Simultaneously, there is pressure to expand and make use of the

16. The conditions are vital in what constitutes legitimate targeting though. Some things – such as critical infrastructure – are strictly off limits in peace time, but become a legitimate target under conditions of war.
17. A possible future candidate for the Hague logic might be fully autonomous cyber-attacks (like the worms of the past but with a much more damaging payload).
18. UN GGE consensus report 2015, arts. 13f and 13k.
19. Dennis Broeders. (2015). *The public core of the internet. An international agenda for internet governance.* Amsterdam: Amsterdam University Press; Global Commission on the Stability of Cyberspace. (2017). *Call to protect the public core of the internet*; see also, the *Paris Call for Trust and Security in Cyberspace.*
20. Review Committee on the Intelligence and Security Services. (2018). "Joint Statement: Strengthening Intelligence Oversight Cooperation", 14 November 2018.

new possibilities the digital domain has to offer in terms of espionage and more aggressive cyber operations. Given that many intelligence agencies outside of the western world are much less constrained by national legislation, states on both sides are reluctant to (unilaterally) limit their options to conduct cyber operations. There is a structural tension between the values-based approach of legislation and the utility and capabilities approach that underlies strategic and operational concerns. Competition among the top tier states carries the risk of sliding into a dynamic of 'fighting fire with fire'. If the American response to Russian influence operations is to 'integrate cyberspace operations with information operations' themselves, the damage to liberal values may easily outweigh operational gains in the longer term. The integrity of information underlies the public debate that sustains the liberal democratic model. Information operations and the spreading of disinformation – operationalising the integrity of information – undercuts those values and opens western states up to charges of hypocrisy and risks escalation. As current international dynamics facilitate escalation – in the sense of driving states to develop cyber operations that will give them an edge – the case for a rules based order for intelligence agencies (ideally internationally) should be made and strengthened. Given the fact that the 'second oldest profession in the world' has mostly eluded domestic control until recent decades, and remained effectively outside of international control up until the present day, this will need to start with a bottom-up approach. The following points offer some initial proposals for policy-makers involved in the field of cyber and international security.

Recommendations

- Resist the temptation of replying in kind to influence operations that target the integrity of public information. Integrity of data and information – much more than confidentiality and availability – touches on core values of democratic societies.
- Explore possibilities to define objects and organisations that should be off limits for cyber operations, in line with the 'Geneva' style of the regulation of responsible state behaviour.
- Rethink and articulate the boundaries between military cyber operations and intelligence cyber operations. Legal frameworks should define those boundaries rather than operational capabilities.
- Build on the trend in many western states that have legally anchored intelligence agencies to the values and the institutions of democracy and the rule of law.
- Explore possibilities to extend and facilitate international cooperation between national oversight structures to mirror the international cooperation of foreign intelligence agencies.

Authors

Dennis Broeders is Associate Professor of Security and Technology and Senior Fellow of The Hague Program for Cyber Norms at the Institute of Security and Global Affairs at Leiden University. Prior to joining Leiden University, he was a Senior Research Fellow at the Netherlands Scientific Council for Government Policy and Professor of Technology and Society at Erasmus University Rotterdam.

Sergei Boeke is a non-resident fellow of Leiden University's The Hague Program for Cyber Norms. Between 2013 and 2019 he was a lecturer/researcher at the Institute of Governance and Global Affairs at Leiden University. He previously worked in the Dutch military, diplomacy and intelligence.

Ilina Georgieva is a PhD candidate of The Hague Program for Cyber Norms. In her research, Ilina is focusing on the capacity of intelligence agencies to propagate cyber norms by means of their conduct in cyberspace, and to thus shape the international community's perception of what is normal in cyberspace. For that purpose she investigates the agencies' normative power by looking into their practice of foreign bulk data collection.

Acknowledgements
The authors would like to thank Karine Bannelier-Christakis, Pieter Bindt, Mark Phythian and Simon Willmetts for their insightful comments on an earlier draft of this policy brief. We would also like to thank Sean Kanuck for his help in organising and running the workshop 'Foreign Intelligence in Cyberspace' that was held in The Hague in April 2019 and for his contribution to the rough outline of this policy brief.

All of the activities and publications of The Hague Program for Cyber Norms are supported by a grant of the Dutch Ministry of Foreign Affairs.

Contact information

E-mail: info@thehaguecybernorms.nl
Website: https://www.thehaguecybernorms.nl
@HagueCyberNorms

Address
The Hague Program for Cyber Norms
Faculty of Governance and Global Affairs
Leiden University
Hague Campus
Turfmarkt 99
2511 DP The Hague

Colofon
Published September 2019.

Graphic design: www.pauloram.nl

THE HAGUE
PROGRAM
for Cyber Norms

Universiteit
Leiden