2019 11th International Conference on Cyber Conflict:
Silent Battle
T. Minárik, S. Alatalu, S. Biondi,
M. Signoretti, I. Tolga, G. Visky (Eds.)
2019 © NATO CCD COE Publications, Tallinn

"Silent Battle" Goes Loud: Entering a New Era of State-Avowed Cyber Conflict

Keir Giles
Conflict Studies Research Centre
Northamptonshire, UK
keir.giles@conflictstudies.org.uk

Kim Hartmann
Conflict Studies Research Centre
Northamptonshire, UK
kim.hartmann@conflictstudies.org.uk

Abstract: The unprecedented transparency shown by the Netherlands intelligence services in exposing Russian GRU officers in October 2018 is indicative of a number of new trends in state handling of cyber conflict. US public indictments of foreign state intelligence officials, and the UK's deliberate provision of information allowing the global media to "dox" GRU officers implicated in the Salisbury poison attack in early 2018, set a precedent for revealing information that previously would have been confidential.

This is a major departure from previous practice where the details of state-sponsored cyber attacks would only be discovered through lengthy investigative journalism (as with Stuxnet) or through the efforts of cybersecurity corporations (as with Red October). This paper uses case studies to illustrate the nature of this departure and consider its impact, including potentially substantial implications for state handling of cyber conflict. The paper examines these implications, including:

- The effect of transparency on perception of conflict. Greater public knowledge of attacks will lead to greater public acceptance that countermeasures should be taken. This may extend to public preparedness to accept that a state of declared or undeclared war exists with a cyber aggressor.
- The resulting effect on legality. This adds a new element to the long-running debates on the legality of cyber attacks or counter-attacks, by affecting the point at which a state of conflict is politically and socially, even if not legally, judged to exist.

- The further resulting effect on permissions and authorities to conduct cyber attacks, in the form of adjustment to the glaring imbalance between the means and methods available to aggressors (especially those who believe themselves already to be in conflict) and defenders. Greater openness has already intensified public and political questioning of the restraint shown by NATO and EU nations in responding to Russian actions; this trend will continue.
- Consequences for deterrence, both specifically within cyber conflict and also more broadly deterring hostile actions.

In sum, the paper brings together the direct and immediate policy implications, for a range of nations and for NATO, of the new apparent policy of transparency.

Keywords: *cyber conflict, cyber policy, attribution, deterrence, transparency*

1. EMERGING PRACTICE

Coordinated disclosures by a number of Western powers of details of cyber attacks and other hostile actions appear to indicate a new multinational policy of state transparency regarding the handling of selected cyber incidents. Combined with the growing power of private citizens and non-governmental organisations engaging in open source intelligence collection and analysis, this may lead to a substantially new phase in the development of cyber conflict.[1]

State cyber activities have traditionally been deeply classified, for a range of reasons including not disclosing either capabilities or vulnerabilities. According to one analysis, “The entire phenomenon of cyber war is shrouded in such government secrecy that it makes the Cold War look like a time of openness and transparency”.[2] And yet, the unprecedented level of detail disclosed by the Netherlands intelligence services in exposing Russian GRU officers in October 2018 signalled a new departure in state handling of cyber conflict. US public indictments of foreign state intelligence officials, and the UK’s release of limited information which enabled third parties to independently identify the Salisbury attackers, set precedents for revealing information that previously would have been confidential, and confirmed a number of new trends in emerging practice.

[1] For an overview of the developmental phases of cyber conflict to date see Max Smeets and Jason Healey, “Cyber Conflict History”, Cyber Conflict Studies Association, 2017, http://static1.1.sqspcdn.com/static/f/956646/28023292/1541729131737/SotF+2017+CCSA+SIPA+History.pdf

[2] R.A. Clarke and R. Knake, *Cyber War: The Next Threat to National Security and What to Do About It* (2010), p. xi

In traditional state practice, a cyber incident would be subjected to a long and painstaking phase of incident analysis before any consideration was given to public attribution. This analysis would include technical evidence as well as supporting material from other sources (historical, geopolitical context, signals and human intelligence and more). The incident analysis would ordinarily be confidential and not available to the public, which might only learn details of the incident through the investigations of private sector cyber security corporations. The second phase, of public or diplomatic attribution by a body or representative of a state, would be considered based on foreign policy considerations as well as on objective evidence. Throughout 2018, however, a shift in practice has been observable as state victims of cyber incidents become increasingly transparent about the details of the investigative phase, whether before or after attribution to a perpetrator: there is increasing disclosure of codes, networks, names, locations, dates, procedures, methodologies, human relationships and relations to other cyber incidents.[3] If this process continues, cyber conflict will change from being a silent battle to one conducted at full volume in the same manner as other forms of state-on-state confrontation.

A general trend towards increased disclosure of cyber incidents in the corporate sector has been noted in the current decade.[4] However, disclosure of state-on-state confrontations increased significantly during 2018 in particular. The Centre for Strategic and International Studies (CSIS) reports on significant cyber incidents on a regular basis, with "significant" meaning attacks carried out "on government agencies, defense and high tech companies, or economic crimes with losses of more than a million dollars".[5] According to the CSIS "Significant Cyber Events List since 2006", during the year 2018, 112 significant cyber incidents were reported, and of these reports almost 45% were official government statements. In addition, these official statements were proactively offering deep insights into the incident detected, the measures taken to counter it, and specific details on the perpetrators.[6] By comparison, for the year 2017 CSIS logged 60 such incident reports, and only 38 in 2016 – and of the 2016 reports, only eight contained any detail over and above simple confirmation that an incident had occurred.

[3] This is partly facilitated by the investigative methods used in technical incidents, which generally include the immediate creation of a "forensic duplicate" of all items involved in the investigative phase. As this guarantees that no evidence from the system can be removed or altered, it allows earlier distribution of investigative results to a broader audience, even prior to the attribution of the incident to a perpetrator. Specifications for forensic duplicates may be found in "Leitfaden IT-Forensik' Version 1.0.1", Bundesamt für Sicherheit in der Informationstechnik (BSI), March 2011.

[4] Derryck Coleman, "Cyber Risk Disclosure On The Rise", Audit Analytics, 23 November 2016, https://www.auditanalytics.com/blog/cyber-risk-disclosure-on-the-rise/; Hilary, Gilles and Segal, Benjamin and Zhang, May H., Cyber-Risk Disclosure: Who Cares? (October 14, 2016). Georgetown McDonough School of Business Research Paper No. 2852519. Available at SSRN: https://ssrn.com/abstract=2852519 or http://dx.doi.org/10.2139/ssrn.2852519

[5] Centre for Strategic and International Studies (CSIS), Significant Cyber Incidents, 9 March 2019, https://www.csis.org/programs/cybersecurity-and-governance/technology-policy-program/other-projects-cybersecurity

[6] Centre for Strategic and International Studies (CSIS), Significant Cyber Incidents full report since 2006, 9 March 2018, https://csis-prod.s3.amazonaws.com/s3fs-public/190211_Significant_Cyber_Events_List.pdf

Emerging state practice also shows that in addition to occurring with higher frequency, transparency efforts are increasingly:

- **Collective:** increasingly, multiple states attribute cyber incidents jointly, and a nascent "transparent cyber alliance" is discernible.
- **Coordinated in policy:** there were at least two instances in 2018 when public release of details of a cyber incident was coordinated with other major political events (see case studies below). This pattern of coordination is reflected in the establishment of political tools and mechanisms, such as the EU Cyber Security Diplomatic Toolbox or NATO Mechanisms for Response.
- **Coordinated in time:** in early October 2018 the British, New Zealand and Australian governments published a list of GRU attacks described as "indiscriminate and reckless cyber attacks targeting political institutions, businesses, media and sport" around the world. Immediately afterwards, the Netherlands authorities released the details of the GRU attempt to hack into the headquarters of the Organisation for the Prohibition of Chemical Weapons in The Hague, detected and interdicted several months before in early April. Finally, on the same day, the US Department of Justice announced criminal charges against seven Russian military intelligence officers.
- **Independent of the scale, nature or impact of the event:** the disclosure of the attempted OPCW hack shows that states do not always consider only the scale and gravity of the operation as a rationale for public attribution, but also the target (as with the OPCW as an international organisation) and the context (the perpetrators involved being also involved in other major cyber incidents).

Key Western allies appear to have shifted to a "public engagement campaign" intended to disrupt and deter cyber attacks and other forms of hostile activity.[7] This is despite the absence of any official national or international statement on change of policy. Explicit policy changes appear limited to very specific types of attack, for instance disinformation attacks on the United States. At the July 2018 Aspen Security Forum, then US Deputy Attorney General Rod Rosenstein seconded a recommendation that the US Justice Department should, under certain circumstances, publicly disclose and attribute foreign influence operations, noting that: "Exposing schemes to the public is an important way to neutralize them" and that "attribution of foreign influence operations can help to counter and mitigate the harm caused by foreign-government-sponsored disinformation." In September of the same year, this became official policy,

[7] Alexander Smith, "Norway calling out Russia's jamming shows European policy shift", *NBC News*, 24 November 2018, https://www.nbcnews.com/news/world/norway-calling-out-russia-s-jamming-shows-european-policy-shift-n937886

as the US Justice Department included a section on "Disclosure of Foreign Influence Operations" as part of an update of the US Attorney's Manual.[8]

Nevertheless, the move to wider public disclosure of the fine detail of cyber incidents is visible in the United States in particular. During late 2018, the pace of detailed US public indictments accelerated notably. In September, US officials indicted a North Korean man for his alleged role in the hack of Sony Pictures studios, almost four years after the attack. In October, seven Russian military intelligence officers were charged with "computer hacking, wire fraud, aggravated identity theft, and money laundering." In early November, indictments were made public against more than a dozen Chinese men accused of hacking American aerospace firms for five years beginning in January 2010.[9] But, as the following case studies show, this trend is accompanied by substantial international cooperation to maximise the effect of transparency.

2. CASE STUDIES

Public attribution of a cyber incident by a state directly accusing another state is not in itself new, and case studies are available from before 2018. In May 2014, the US Department of Justice indicted five officers of China's Unit 61398 for commercial theft in the US;[10] and in February 2015 Norway publicly accused China of commercial cyber espionage and use of the stolen data for the development of new military technology. But 2018 represented a watershed in the frequency, transparency, and method of delivery of public attribution. In addition to the instances already mentioned, in February NotPetya was publicly attributed to the Russian Federation by the UK, Denmark, the US, Canada, Australia and New Zealand, later supported by Estonia, Latvia, Lithuania, Finland and Sweden. In April Germany publicly accused Russia of a cyber attack on the IVBB government data network.[11] In mid-July the US charged 12 GRU officers with a range of offences connected with attacks on the 2016 presidential election.[12] And in October the UK Foreign Office issued a statement in which it jointly with Microsoft accused the Lazarus group, supported by the DPRK, of the WannaCry attack. This attribution was later supported by the US, Canada, New Zealand and Japan. Finally for the year, in late December the US announced a further

[8] Eliot Kim, "Summary: Justice Department Policy on 'Disclosure of Foreign Influence Operations'", *Lawfare*, 16 October 2018, https://www.lawfareblog.com/summary-justice-department-policy-disclosure-foreign-influence-operations

[9] Ben Watson, "Special Report: Is the US Ready to Escalate in Cyberspace?" *Defense One*, 21 November 2018, https://www.defenseone.com/ideas/2018/11/special-report-us-ready-escalate-cyberspace/153001/

[10] "U.S. Charges Five Chinese Military Hackers for Cyber Espionage Against U.S. Corporations and a Labor Organization for Commercial Advantage", Department of Justice, 19 May 2014, https://www.justice.gov/opa/pr/us-charges-five-chinese-military-hackers-cyber-espionage-against-us-corporations-and-labor

[11] "Moscow likely behind hack on German govt, spy chief says", Reuters, 11 April 2018, https://www.reuters.com/article/us-germany-security/moscow-likely-behind-hack-on-german-govt-spy-chief-says-idUSKBN1HI19D

[12] Indictment available at https://www.justice.gov/file/1080281/download

round of sanctions in retaliation for cyber attacks and “other malign activities,”[13] and the US and UK jointly accused China of a long-running campaign of intellectual property theft, in disclosures backed by Australia and New Zealand and seen as signalling “growing global coordination against the practice.”[14]

Amid this accelerating pace of disclosures, late September and early October 2018 saw two instances which exemplified all the new features of the apparent internationally coordinated policy of transparency over hostile actions. In September the British government disclosed details of the two suspects in the poisoning of Sergey and Yuliya Skripal in Salisbury, UK. The next day saw a debate in the United Nations Security Council, initiated by the UK, which must have been preceded by a long period of painstaking multilateral diplomatic preparation. In prepared statements the leaders of the United States, France, Germany and Canada backed Britain’s assessment,[15] while a round of statements from countries represented on the Security Council either condemned Russia or were cautiously equivocal, depending on how much each country had to lose from falling out with Moscow. More than 20 countries subsequently supported the UK in its allegations against Russia, expelling more than 100 Russian diplomats between them.

A month later, a similar degree of international coordination over disclosures was evident in the release by the Netherlands of highly detailed information on the interdiction of an attempted hack of the Organisation for the Prohibition of Chemical Weapons in The Hague in the previous April.[16] Near simultaneous announcements were made by the UK and US. A British government statement delivered by the UK Ambassador to the Netherlands promised further public action in close cooperation with allies “confronting, exposing and disrupting the GRU’s activity.”[17] And on the same day, the US charged seven GRU officers with hacking and other offences related to a report on Russia’s systematic state-sponsored subversion of the sport drug-testing process. Four of the seven had travelled to The Hague to carry out the attempted cyber attack on the OPCW, and three had also been indicted in relation to attacks on the US presidential election. As in other instances, the indictment contained highly detailed

[13] “Treasury Targets Russian Operatives over Election Interference, World Anti-Doping Agency Hacking, and Other Malign Activities”, U.S. Department of the Treasury, 19 December 2018, https://home.treasury.gov/news/press-releases/sm577

[14] “U.S., allies slam China for economic espionage, spies indicted”, Reuters, 20 December 2018, https://www.reuters.com/article/us-china-cyber-usa/u-s-allies-slam-china-for-economic-espionage-spies-indicted-idUSKCN1OJ1VN

[15] Angela Dewan and Nada Bashir, “World leaders back UK’s Novichok nerve agent allegations against Russia”, *CNN*, 6 September 2018.

[16] “Netherlands Defence Intelligence and Security Service disrupts Russian cyber operation targeting OPCW”, Government of the Netherlands, 4 October 2018, https://www.government.nl/latest/news/2018/10/04/netherlands-defence-intelligence-and-security-service-disrupts-russian-cyber-operation-targeting-opcw

[17] “Minister for Europe statement: attempted hacking of the OPCW by Russian military intelligence”, UK Government, 4 October 2018, https://www.gov.uk/government/speeches/minister-for-europe-statement-attempted-hacking-of-the-opcw-by-russian-military-intelligence

descriptions of the activities of individual GRU officers, identifying fake accounts and domain names and the precise times and locations of specific online activities.[8]

The involvement of the US and the UK in both incidents reflects a shared perception of the Russian challenge in both governments. In the US this indicates recognition of the wide range of cyber threats emanating from Russia,[19] and in particular the broad range of hostile activities undertaken against the United States, including for example against key utilities and infrastructure.[20] And a new readiness by senior figures in the UK to publicly recognise and state the challenge of ongoing offensive cyber activity from Russia had been discernible from early 2018.[21] The heightened willingness of British intelligence agencies to respond firmly to Russia may account for later reports that a long-serving Russian spy in the Austrian armed forces was arrested on the basis of information provided by the UK.[22]

3. EFFECTS AND IMPLICATIONS

A policy of transparency has a range of implications beyond the possible immediate aim of deterring hostile cyber actors. Before considering deterrence itself, this section highlights potential second- and third-order effects of more open handling of cyber incidents.

A. Legality in Cyberspace

The result of greater publicity for cyber incidents is not only to turn up the volume on a previously silent battle. It also transforms cyber conflict from being invisible to being apparent and tangible. Details disclosed by states based on intelligence sharing/gathering or sophisticated investigations make cyber conflict comprehensible and real rather than an abstraction that publics find difficult to imagine and to relate to their own lives. This could add a new element to the long-running debates on the legality of cyber attacks or counter-attacks, by affecting the point at which a state of conflict is politically and socially, even if not legally, judged to exist.

[18] "U.S. Charges Russian GRU Officers with International Hacking and Related Influence and Disinformation Operations", US Department of Justice, 4 October 2018, https://www.justice.gov/opa/pr/us-charges-russian-gru-officers-international-hacking-and-related-influence-and

[19] Nicu Popescu and Stanislav Secrieru (eds.), "Hacks, Leaks and Disruptions: Russian Cyber Strategies", Chaillot Papers No. 148, October 2018, https://www.iss.europa.eu/sites/default/files/EUISSFiles/CP_148.pdf

[20] Rebecca Smith and Rob Barry, "America's Electric Grid Has a Vulnerable Back Door—and Russia Walked Through It", *The Wall Street Journal*, 10 January 2019, https://www.wsj.com/articles/americas-electric-grid-has-a-vulnerable-back-doorand-russia-walked-through-it-11547137112

[21] Lizzie Dearden, "Britain has entered 'new era of warfare' with Russian cyber attacks, Defence Secretary warns", *The Independent*, 15 February 2018, https://www.independent.co.uk/news/uk/home-news/russia-cyber-attacks-notpetya-gavin-williamson-defence-secretary-putin-hacking-ransomware-a8212801.html

[22] Michael Jungwirth, "Britischer Geheimdienst ließ Putins Spion in Österreich auffliegen", *Kleine Zeitung*, 11 November 2018, https://www.kleinezeitung.at/politik/aussenpolitik/5528189/Der-Tipp-kam-aus-London_Britischer-Geheimdienst-liess-Putins-Spion

Invocation of the principles of international humanitarian law in cases of cyber conflict remains rare. Only a few states have been explicitly clear about the application of international law in cyberspace: once again the UK,[23] the US and the Netherlands. And the division persists between the Western view of the applicability of international law in cyberspace, and that held by Russia, China and like-minded nations, despite a slowly evolving normative debate. Even where states have engaged in international forums on cyber norms (UN GGE, the Global Commission on the Stability of Cyberspace, regional organisations, the OSCE and more) there is an apparent reluctance to adopt an open position on what is lawful in cyberspace and what is not. This is partly due to considerations among states that consider themselves bound by the rule of law not to set a threshold below which an adversary can attack without fear of countermeasures.

But even if states do not explicitly invoke international law when publicly attributing or indicting individuals for cyber attacks, the rationale behind 'going loud' and the emerging State practice is to show that malicious cyber operations

- are not acceptable;
- will not remain secrets kept only by the respective intelligence communities; and
- will incur consequences (even if the eventual consequences or countermeasures if there is no prospect of prosecution of indicted individuals remain to be seen).

In general, open, transparent and public condemnation of incidents demonstrate states' understanding of legality in cyberspace, and their understanding of what constitutes unlawful behaviour. This assumption does not entirely work *a contrario*: if a state does not engage in naming and shaming, this does not mean that it perceives the cyber incident in question as legal, but perhaps it has not yet or fully determined its position on regulation in cyberspace – or indeed does not possess the capability to attribute clearly at any level. Nevertheless, overall a greater adoption of transparency must accelerate the development of international customary law, by forcing open and public consideration of specific documented instances rather than abstract and hypothetical studies.

B. Permissions and Authorities

The reluctance of states to commit to specific interpretations of legality in cyberspace leaves open the argument that cyber operations take place in a grey zone of legal ambiguity.[24]

[23] "Cyber and International Law in the 21st Century", UK Government website, 23 May 2018, https://www.gov.uk/government/speeches/cyber-and-international-law-in-the-21st-century

[24] Kubo Mačák, "From Cyber Norms to Cyber Rules: Re-engaging States as Law-makers", *Leiden Journal of International Law* (2017), 30, pp. 877–899, doi:10.1017/S0922156517000358

At the same time, increased state transparency on cyber and other incidents will inevitably lead to greater public knowledge of attacks, and develop a broader consciousness of a state of ongoing conflict by highlighting instances of state-sponsored hostile action. This may start to redress the striking imbalance in public consciousness between aggressors and defenders. This is particularly marked in the case of countries such as Russia, whose state media has been promoting war rhetoric for almost a decade and whose population is constantly reminded that their country is in conflict with the West and that the internet presents a means through which the West can attack and subvert Russia.[25] By contrast, Western countries' publics are only dimly and intermittently aware that Russia wishes them harm.

In this case, public pressure for retaliatory measures may grow. In particular, public and political questioning of the restraint shown by NATO nations in responding to hostile actions by rogue states will intensify still further. This may in turn lead to adjustments to the restrictions on Western cyber and other agencies, whose permissions and authorities to take action generally presume a state of peace, and consequently are greatly more constrained than those of their adversaries. In short, if publics and policy-makers are more aware that war is being waged against them, whether declared or not, they are more likely to favour responses in kind.

Indicators of this kind of movement are already visible on the national and supranational levels. In the US, some of the restrictions governing the approval process for offensive cyber attacks against adversaries were lifted in September 2018,[26] accompanying a strategic reorientation in cyber described as "defend forward."[27] NATO declaratory policy, too, allows "responding in a coordinated manner" to attributed malicious cyber activity.[28]

C. Deterrence

These types of measures may in the medium term enhance the capability of Western nations to implement effective deterrence in cyberspace. For now, public identification of perpetrators, even if accompanied by indictments, is of limited effect if those perpetrators are unlikely ever to be present in a jurisdiction where they could be arrested and tried. Consequently the primary value of transparency at present is in combating the perceived anonymity and immunity of cyber operations;[29] in the US in

[25] Kim Hartmann and Keir Giles. "Net neutrality in the context of cyber warfare", *2018 10th International Conference on Cyber Conflict (CyCon)*. IEEE, 2018.

[26] Erica Borghard and Shawn Lonergan, "What Do the Trump Administration's Changes to PPD-20 Mean for U.S. Offensive Cyber Operations?" Council on Foreign Relations, 10 September 2018, https://www.cfr.org/blog/what-do-trump-administrations-changes-ppd-20-mean-us-offensive-cyber-operations

[27] Max Smeets and Herb Lin, "An Outcome-Based Analysis of U.S. Cyber Strategy of Persistence & Defend Forward", *Lawfare*, 28 November 2018, https://www.lawfareblog.com/outcome-based-analysis-us-cyber-strategy-persistence-defend-forward

[28] "Brussels Summit Declaration", NATO, 11 July 2018 https://www.nato.int/nato_static_fl2014/assets/pdf/pdf_2018_07/20180713_180711-summit-declaration-eng.pdf

[29] Jory Heckman, "WH cybersecurity coordinator seeks more 'naming and shaming' of hackers", *Federal News Network*, 29 January 2018, https://federalnewsnetwork.com/cybersecurity/2018/01/wh-cybersecurity-coordinator-seeks-more-naming-and-shaming-of-hackers/

particular, this follows recognition that the Obama administration's muted response to Russian attacks on the US democratic process during the 2016 presidential election was counterproductive, and encouraged Russia in the belief that it could carry out further attacks with little risk of adverse consequences. A secondary effect is to allow less complicated sharing of cyber intelligence; once the information is declassified and publicly available, there are no constraints on passing it on to third-party victim states, or to the media or private sector security corporations in order to assist their own investigations. Each of these actions will have its own deterrent effect.

But critics argue that there is little point in naming and shaming a perpetrator that feels no shame. Indeed in some cases Russia in particular may be appreciative of the publicity, since "just as with so many other aspects of Moscow's geopolitics, there is a theatrical aspect… as the country tries to assert an international status out of proportion with the size of its economy, its soft power and arguably even its effective military strength."[30] This suggests that the prospect of further and more substantive countermeasures may be required in order to deliver deterrence, and it is this consideration which probably lies behind public announcements that the UK had "war-gamed a massive cyber-strike to black out Moscow if Vladimir Putin launches a military attack on the West",[31] followed shortly by similar messaging from the US.[32]

In the US at least, the new policy of transparency has extended in at least one case to acknowledging countermeasures. Instances of operations in cyberspace that are combined with overt and public acknowledgement by the perpetrator are exceptional; ordinarily if there is any accompanying messaging it is kept strictly confidential, and in public responsibility is vehemently denied. The US is now tracing back and directly contacting individuals engaging in online disinformation operations on behalf of the Russian state, with the aim of overtly warning them they could be personally liable to public exposure, indictment, and sanctions from the US government.[33] This departure from anonymity constitutes a striking precedent, which if extended to other forms of cyber operation could substantially change how governments view the delivery of cyber effects.[34]

[30] Mark Galeotti, "Heroes of the Fatherland: Killing Here, Hacking There", *The Moscow Times*, 25 December 2018, https://themoscowtimes.com/articles/heroes-of-the-fatherland-killing-here-hacking-there-63901

[31] Caroline Wheeler, Tim Shipman and Mark Hookham, "UK war-games cyber attack on Moscow", *The Sunday Times*, 7 October 2018, https://www.thetimes.co.uk/article/uk-war-games-cyber-attack-on-moscow-dgxz8ppv0

[32] "The Pentagon has prepared a cyberattack against Russia", *Daily Beast*, 2 November 2018, https://www.thedailybeast.com/the-pentagon-has-prepared-a-cyber-attack-against-russia

[33] Sean Gallagher, "Russian trolls get DM from US Cyber Command: We know who you are. Stop it", *Ars Technica*, 23 October 2018, https://arstechnica.com/information-technology/2018/10/us-cyber-command-doxes-dms-warnings-to-russian-disinformation-trolls/

[34] Evan Perkoski and Michael Poznansky, "CyberCom Is Targeting Russia's Election Meddlers — and Changing How Governments Use Cyber", *Defense One*, 31 October 2018, https://www.defenseone.com/ideas/2018/10/cybercom-targeting-russias-election-meddlers-and-changing-how-governments-use-cyber/152455/

4. OUTLOOK AND CONCLUSIONS

In early 2019, the ongoing efforts of the Netherlands to name the perpetrators of state-sponsored hostilities appeared to be continuing. Importantly, this trend is not limited to cyber activities, but extends to other domains as well. In January, for instance, the Dutch government accused Iran of involvement in at least four assassination and bomb plots in Europe since 2015, and disclosed that investigations into two killings in the Netherlands had led to the expulsion of two Iranian diplomats in June 2018, a move that was not disclosed at the time.[35]

But the trend toward transparency in any domain should not be expected to proceed smoothly and without checks and reverses. One constraint on future application may be concern at the prospect of reprisals. One analysis of recent US moves holds that the response to Russia's information offensive has been deliberately restrained, "in large part to keep Moscow from escalating in response by taking down the power grid or conducting some other reprisal that could trigger a bigger clash between great powers."[36] Another significant risk is horizontal escalation, in particular when dealing with states that are willing to apply whole-of-government measures to attacking their adversaries. For instance, public attribution of cyber attacks that have been carried out by states with limited domestic application of the rule of law may lead to reprisals against private individuals. Both Russia and China have demonstrated willingness to retaliate against Western countries by targeting their citizens resident in or visiting those countries. In Russia, at the time of writing, joint US-British-Irish-Canadian citizen Paul Whelan was being held in apparent retaliation for the arrest in the United States of the Russian alleged agent of influence Maria Butina.[37] In China, larger numbers of Canadians have been detained following the arrest in Canada of Huawei Chief Financial Officer Meng Wanzhou.[38] US citizens are also affected by similar measures there. With effect from January 2018, US citizens travelling to China are advised to "exercise increased caution in China due to arbitrary enforcement of local laws," in particular the coercive use of "exit bans" to prohibit individuals from leaving China, sometimes keeping US citizens in China for years.[39]

[35] Adam Taylor, "Did Iran plot four attacks in Europe? The Dutch government thinks so", *The Washington Post*, 8 January 2019, https://www.washingtonpost.com/world/2019/01/08/did-iran-plot-attacks-europe-dutch-government-thinks-so/

[36] Julian Barnes, "U.S. Begins First Cyberoperation Against Russia Aimed at Protecting Elections", *The New York Times*, 23 October 2018, https://www.nytimes.com/2018/10/23/us/politics/russian-hacking-usa-cyber-command.html

[37] Catherine Philip and Tom Parfitt, "British citizen Paul Whelan held in Russia over 'spying for the West'", *The Time*s, 4 January 2019, https://www.thetimes.co.uk/edition/news/british-citizen-paul-whelan-held-in-russia-over-spying-for-the-west-ghglb88kw

[38] "Canada says 13 citizens detained in China since Huawei CFO arrest", Reuters, 4 January 2019, https://www.reuters.com/article/us-usa-china-huawei-tech-idUSKCN1OY05Q

[39] "China Travel Advisory", U.S. Department of State, 3 January 2019, https://travel.state.gov/content/travel/en/traveladvisories/traveladvisories/china-travel-advisory.html

States may choose to withhold public attribution even when confident in their findings and confident that the risk of reprisals can be avoided or mitigated. This means that selective application of transparency and disclosure should allow a calibrated response to cyber incidents. But in all cases, responses in an environment of greater public consciousness will require extremely close coordination between intelligence services, policy-makers, and the deliverers of cyber effects.[40]

State disclosures will not replace the role of non-state actors, whether information security corporations for cyber incidents, investigative journalism for hostile actions in other domains, or a mixture of the two and more. US indictments, and the release by the UK of limited information on the suspects in the Skripal attack, gave independent media and non-governmental investigators the leads required to develop a much clearer picture of the individuals and structures involved in hostile actions.[41] This harnessing of the power of the global media will serve an important function in bringing vulnerabilities to foreign attack to public notice in the victim state, while not compromising confidential sources or legal process by releasing classified information.

In addition, there will be second- and third-order effects of a new policy of open accusations of hostile acts by states that may as yet be imperfectly understood. One such example is in insurance against cyber attack and its consequences; if it is established that an incident was a state-on-state (and especially military) attack, rather than one carried out by criminals in the traditional sense, this will invalidate a whole range of insurance policies. The result could be substantial disruption to the business insurance market, as corporations look for insurance that does not exclude hostile cyber acts.[42]

Finally, and critically, the trend of greater public awareness is not limited to cyber activity or to disclosures by states. In December 2018, President Trump’s inability to undertake a trip to Iraq in secret underscored the democratisation of detection of a wide range of formerly confidential government activity. Mass communications, crowdsourcing, and the widespread availability of open source intelligence analysis tools mean that “The era of spy versus spy—if it ever truly existed—has certainly been ended… Today it is spy versus tweeter, plane spotter, criminal, activist, journalist, bored teenage hacker, and who knows who else.”[43] The result is that in

[40] As described in Max Smeets, “Integrating offensive cyber capabilities: meaning, dilemmas, and assessment”, *Defence Studies*, Volume 18, 2018 - Issue 4, pp. 395-410, DOI: 10.1080/14702436.2018.1508349

[41] See for example “Investigative Report: On the Trail of the 12 Indicted Russian Intelligence Officers”, *RFE/RL*, 19 July 2018, https://www.rferl.org/a/investigative-report-on-the-trail-of-the-12-indicted-russian-intelligence-officers/29376821.html

[42] Oliver Ralph and Robert Armstrong, “Mondelez sues Zurich in test for cyber hack insurance”, *Financial Times*, 10 January 2019, https://www.ft.com/content/8db7251c-1411-11e9-a581-4ff78404524e

[43] James Ball, “Plane Enthusiasts Spy Air Force One, Reveal Trump’s Secret Trip”, *The Atlantic*, 28 December 2018, https://www.theatlantic.com/amp/article/579151/

those cases where governments determine that transparency is not the desired option and they wish to keep their enterprises silent, they will be forced to adopt an entirely new approach to measures to protect and disguise activities that otherwise will be conducted in public.[44] This also has implications for deterrence and its applicability to cyber activities. Previously it might have been possible to engage in deterrence by punishment, or simply assertive messaging, by undertaking a cyber operation that was comprehensible to the adversary but invisible to the general public, so the conspiracy of silence between the aggressor and victim would make it possible for the message to be received with no further escalatory retaliation.[45] Now, it may no longer be possible to message or punish privately and expect the incident to remain confidential for long. In short, in cyber operations, as in so many other areas of previously covert state activity, secrets will have a half-life.

Acknowledgement

The authors thank Berta Jarosova for her research contribution to this paper.

[44] Ric Cole, "Rethinking Camouflage", *Medium*, 15 October 2018, https://medium.com/@richard_iain_cole/rethinking-camouflage-74efadf14ff7

[45] Explored in detail by Austin Carson in *Secret Wars: Covert Conflict in International Politics*, Princeton University Press, 2018.