DOI:
10.1080/23738871.2021.2000628

Document Version
Peer reviewed version

On the Strategic Consequences of Digital Espionage

Joe Devanny, Ciaran Martin and Tim Stevens

Corresponding author: tim.stevens@kcl.ac.uk

Abstract

Digital espionage has Cold War origins, but states are still determining how to respond when they are found to be its latest victims. In multilateral discussions about norms of responsible state behaviour in cyberspace, digital political espionage is the elephant in the room. Like other aspects of inter-state intelligence competition, digital espionage is 'business as usual' but can also lead to tensions, particularly when operations become public. The strategic consequences of digital espionage appear significant, as asymmetries of state power and poor understanding of technical aspects of cyber operations lead to uncertainty about appropriate responses to 'cyber victimhood'. We offer multiple propositions to frame state responses to digital espionage, focusing on the relational power of the victim and spying states and their bilateral relationships. States will generally respond proportionately to state-on-state digital espionage, whilst domestic political factors pressure them to adopt more robust, cost-imposing measures that may exacerbate the strategic consequences of digital espionage. We illustrate these propositions with three recent cases – the Snowden revelations (2013); the Office of Personnel Management breach (2014); the SolarWinds breach (2020) – and explore the importance of calibrated responses to digital political espionage for strategic stability and state behavioural norms in cyberspace.

Keywords

Cyber Espionage; Digital Espionage; Cyber Norms; Intelligence Studies.

Introduction

Digital espionage has Cold War origins, but states are still figuring out how to respond to public revelations that they have become its latest victims. Computer network (cyber) capabilities have impacted significantly on multiple dimensions of the intelligence profession – from collection and analysis to effects operations – although whether this constitutes a 'revolution in intelligence affairs' is open to discussion (Gioe et al. 2020). It is now common to observe a significant cyber dimension to contemporary inter-state competition in the 'grey zone' below the threshold of armed conflict, raising ethical and strategic questions about cyber operations and their shaping effect on norms of state behaviour in cyberspace (Martin 2020; Devanny 2020).

This article focuses on one aspect of contemporary cyber competition: the problem of how states respond to being targets of digital espionage, i.e., to being targets of intelligence collection operations exploiting access to digitised data, whether data at rest or in transit over the global 'network of packet-switched networks that comprises the Internet' (Omand 2015, 2). This is related to but distinct from the issue of how states should counter hostile digital information operations (Schia and Gjesvik 2020). Governments come under pressure, in internal policy debates and from the media and interest groups, to respond more assertively after becoming victims to digital espionage than following other types of espionage, such as a major human intelligence (HUMINT) incident. Particularly with HUMINT, this might be due to wide historical familiarity with the dynamics of spying and counter-spying, including an established script for how to respond: declaratory rhetoric and the expulsion of intelligence officers from the relevant embassy. Additionally, the dual-use character of computer network exploitation increases anxiety. Access enabling intelligence collection can be repurposed to conduct offensive cyber operations (computer network attack); exploratory activities for both can look identical (Buchanan 2016). This alone, however, cannot explain the competitive dynamic in contemporary digital espionage that threatens to undermine multilateral efforts to promote responsible state behaviour in cyberspace. Whilst high-level diplomatic discussions have for many years focused on economic cyberespionage by major actors like China, any emerging or novel regime for modulating state cyber activities must take account of, if only to reject, the regulation of political espionage conducted by state parties.

We focus on the strategic consequences of three instances of high-profile digital political espionage to explore their impact on evolving patterns of state responses and the extent to which those responses cut across or contribute to the development of global cyber norms: the 2013 Snowden revelations; the 2015 Office of Personnel Management breach; and the 2020 SolarWinds compromise that affected multiple US federal agencies and departments. We argue that the historically fragile and tacit norms governing inter-state espionage have been unreliable guides to the factors shaping states' responses to major incidents of digital espionage. In calibrating these responses, we argue that 'victim' states should adopt coherent principles of assessment considering: the adversary state's intentions; the system effects of the victim state's own intelligence operations; and the possibility that espionage leads not only or always to state advantage, but also to potential reassurance as a form of confidence-building measure. Digital espionage might therefore enhance rather than reduce strategic stability, but only if victim states acknowledge this and restrain from deliberate escalation. Inter-state intelligence diplomacy – in additional to conventional cyber diplomacy – is essential to the maintenance of equilibrium, the avoidance of cross-domain escalation, and the vitality and prospects of multilateral efforts to foster responsible state behaviour in cyberspace.

This article proceeds in three sections. The first puts responses to publicly exposed cases of digital espionage in strategic context, outlining how they compare to state reactions to human intelligence operations. HUMINT is preferred to the more intuitive comparator of signals intelligence (SIGINT) because its rich history provides more analytical purchase for the exploration of the strategic context of espionage victimhood and specifically victims' responses. From this we extract five propositions about victim states' responses to digital espionage that we then illuminate through narrative descriptions of three US-focused case studies: the Edward Snowden disclosures of 2013; the Office of Personnel Management breach (2014); and the SolarWinds campaign revealed in 2020. Each shows differing state responses to digital espionage through forms of political rhetoric, invocations of domestic and international law, economic sanctions, diplomatic interaction and shifts in strategic posture. In our final analysis, we conclude that states have responded to 'cyber victimhood' in diverse ways. Some, like the United States, invoke the rhetoric of 'imposing costs', in combination with other measures (implicitly including their own cyber operations). Others,

such as the alleged victims of US and allied digital espionage campaigns revealed by Snowden, respond in much more muted fashion. This provisionally supports our central proposition that state responses to cyber victimhood depend significantly on the strategic – and particularly bilateral – context in which the incident manifests. Contemporary global cyber diplomacy rightly focuses on shaping norms of responsible state behaviour in cyberspace. Given its strategic implications, digital espionage and the playbook of state responses should form part of this effort, either directly or in an intelligence-diplomacy complementary to the main effort.

Digital Espionage in Context

States spy on each other. Human intelligence (HUMINT), in which intelligence is gathered through human agency and interaction, was professionalized in the twentieth century but has a much longer and richer history (Scott 2013; Hitz 2004). This history includes many instances in which states have uncovered and remediated penetration cases involving human agents. Standard responses include the expulsion of intelligence officers from embassies and the incarceration of foreign spies. The Cold War also saw the growth of 'spy swaps', in which reciprocal exchanges were coordinated as a calibrated means of managing bilateral tensions and improving stability. These still occasionally take place, such as shortly after the arrest of ten Russian 'illegals' in the United States in June 2010 (Lefebvre and Porteous 2011). In HUMINT situations, therefore, costs are imposed through reputational damage and operational friction, as in declaring embassy staff *personae non gratae* and expelling them from one's jurisdiction. These actions tend to be proportionate – often strictly so – and provisional, as when numbers of embassy intelligence officers are permitted to rise once the initial furore has abated. In some cases, there is tension and uncertainty about the potential strategic ramifications of specific HUMINT operations, which may not attract approval, or for which regret is expressed retrospectively. For example, the head of East German intelligence reportedly came to regard the penetration of West German Chancellor Willy Brandt's private office as a strategic error (Wolf 1997, 171-172). Its exposure led to foreseeable adverse domestic political consequences (resignation) for Brandt. This was a negative development for East Germany and the Soviet Union, who considered Brandt a more palatable head of government than his actual (or any likely) successor.

This indicates that strategic risk calculations about espionage operations are integral to the authorisation process. These focus not only on the likely direct bilateral consequences of an operation's discovery but also on indirect consequences. These might include domestic political effects in the victim state that could lead to less favourable outcomes for the state actor responsible for the espionage operations. A contemporary digital espionage operation provides an interesting counterpoint to the Brandt case. Edward Snowden's disclosures revealed that the US government reportedly intercepted the telephone conversations of German Chancellor Angela Merkel (Traynor and Lewis 2013). This caused public controversy in Germany, but there was no suggestion that Merkel should resign. Unlike Brandt, Merkel's personal judgement was not brought into question: she was an unwitting target of an arm's-length operation. This implies that digital espionage might be interpreted as less strategically destabilising than HUMINT.

The historical record shows that political and diplomatic consequences following public revelations of HUMINT fall into two principal categories. One, they are specific and domestic, as in Brandt's political embarrassment and resignation, and the incarceration of his secretary, Gunther Guillaume, the East German agent responsible. Two, they are managed through proportionately bounded diplomatic interactions. These include 'tit-for-tat' exchanges between adversaries but also periods of strained relations between close allies, as with the US and Israel after the arrest of Jonathan Pollard in 1985 (Lukoff 2018). States generally avoid escalatory spirals and observe conventions sufficiently over time for any breach to be striking, such as the 2018 attempted murder of exchanged Russian military intelligence officer (and British agent) Sergei Skripal (Urban 2018).

Can similar observations be made of digital espionage? Specifically, does emerging state practice resemble a playbook of response options in the wake of public revelations of becoming victim to digital espionage? There is extensive scholarship on the impact of digital technologies on espionage (Pepper 2010; Resnyansky 2010; Warner 2017; Gioe et al. 2020), including HUMINT (Gioe 2017), and on the role and reform of oversight and regulatory arrangements (Omand and Phythian 2018; Cayford et al. 2018; Gill 2020). There is also vigorous discussion of the status of digital political espionage in international law. Broadly, whether one perceives digital espionage as a) not explicitly prohibited under international law and therefore tolerated, particularly if it contributes to strategic stability, or b) as

indirectly prohibited by principles of non-intervention and territorial sovereignty and therefore legitimising countermeasures (Buchan 2019). These debates are important, but the international community is a long way from resolving the legality or otherwise of digital political espionage and attendant countermeasures. We are therefore less concerned here with why states conduct and justify digital political espionage than with how (and how effectively) they respond to being the victim of the digital espionage activities of others. We wish to explore, first, the strategic and domestic political factors shaping states' responses, beyond blanket assertions of the harms of digital espionage and the need for firm and overt counteractions. Second, we examine how state responses to digital espionage might shape and promote responsible state behaviour in cyberspace that emphasises stability and de-escalation.

The discovery of HUMINT cases can lead to strong political rhetoric, as well as profound consequences for an agent in custody (or within reach) of the victim state. Despite that, there is rarely a HUMINT analogue to the 'cost imposition' mantra often heard when digital espionage is uncovered. Nor is there a HUMINT equivalent to the conflation of digital espionage with 'cyber attacks', or their stated correspondence with 'acts of war' or 'warlike activities'. These are common responses to digital espionage, but is there any reason to expect states to react differently to digital espionage than to other forms of espionage such as HUMINT operations? Additionally, 'hacking' is an incontestably salient trope in the contemporary public sphere, driven by real and imagined state and non-state actions, from fear of a 'Cyber Pearl Harbor' to the recent sharp global increase in ransomware crime. This arguably shapes perceptions about the threat of digital espionage, as compared with more conventional – 'passive' – signals intelligence (SIGINT), even if the distinction is underpinned, to a certain degree, by hyperbolic commentary.

Might there potentially be more severe repercussions associated with digital espionage than with other forms of espionage? Even if there is reason to suspect that misunderstanding of the intent (espionage or offensive cyber) behind an operation might lead to escalation (Jervis 2016; Healey and Jervis 2020), this might be less significant than if important constituencies of opinion are primed to react to revelations in potentially escalatory fashion. This highlights two other aspects of the problem. One, that credible inter-state communications about capabilities and intent are sub-optimal. Two, that a government's

freedom of manoeuvre in response to digital espionage victimhood is constrained by domestic reception – led by legislators and sections of the media – such that 'tougher', more escalatory responses are encouraged. Good bilateral communications are therefore essential, but so too is more nuanced public understanding of digital espionage, given the potentially adverse strategic impact of domestic political pressures pushing for escalatory responses, notwithstanding the opportunities potentially afforded to a creative state by framing their response as part of a 'two-level game' (Putnam 1988). This applies also to influential persons whose lack of appreciation of the technical differences between cyber operations leads them to use the misleading language of 'attack' rather than 'espionage'. Our analysis is therefore offered as a contribution to improved understanding of how states have responded to digital espionage victimhood. We hope to encourage further work looking at these issues and their implications both for strategic interaction and for norms of responsible state behaviour.

In multilateral diplomatic efforts to develop norms of responsible state behaviour in cyberspace, digital espionage is one of the weightiest elephants in the room – in Wight's (1977, 30) phrase, a 'reverse image' or 'dark underside' of normal inter-state relations. States often express two apparently incompatible positions. One, commitments in good faith to voluntary, non-binding norms of responsible state behaviour, including ICT supply chain assurance, conscientious vulnerability disclosure, and pursuit of a global cybersecurity culture (UN GGE 2021). Two, the development, acquisition and deployment of 'zero day' exploits to maintain national advantage in digital espionage, online information operations and offensive cyber operations (Martin 2020; Perlroth 2021). Major powers are embracing the multilateral process to develop norms of responsible state behaviour in cyberspace and continue to invest significantly in cybersecurity, including capacity-building for less-capable states (Homburger 2019; Pawlak and Barmpaliou 2017). Some have also explained their vulnerabilities equities processes whilst emphasising the centrality of defensive cybersecurity (Daniel 2014; Aitel and Tait 2016; GCHQ 2018). However, these activities sit uneasily with the persistence and acceleration of inter-state cyber competition, whether for espionage or offensive purposes. As there is potentially a mismatch between operational intent and its interpretation by a target, there is in principle a risk that digital espionage operations could provoke escalation within and beyond cyberspace (Jervis 2016; Healey and

Jervis 2020; Libicki and Tkacheva 2020; Whyte 2020). This elevates the strategic significance of the question of whether there are – or could be – norms of responsible behaviour for state victims of digital espionage.

We assume that HUMINT cases offer initial analytical purchase and offer the following propositions about state responses to becoming victims of targeted digital espionage. We expect (1) victim states to respond proportionately and specifically in these circumstances. This might include personnel exchanges and targeted reputational and personal costs through coordinated attribution and indictments of named individuals. We also expect (2) diplomatic and domestic political contexts to exert shaping effects on victim states responses. Where digital espionage occurs in circumstances of geopolitical competition and has been perpetrated by a major adversary, we expect domestic calls for a strong response but careful calibration of responses by governments mindful of stability and recognising the ubiquity of inter-state espionage. Conversely, just as the US government responded less sternly to Israel following the Jonathan Pollard case than it might in other instances – considering the bilateral relationship and its status in domestic US politics – we would also expect (3) that digital espionage between friendly states attract fewer or less severe repercussions. Similarly, where there are clear asymmetries in relational power, we expect (4) that less powerful victim states will refrain from provocative or escalatory responses, and that (5) more powerful victim states will respond more vigorously to less powerful perpetrating states. We purposely distinguish between states' responses in circumstances of public revelation and those in which breach discovery might yet be prevented from becoming public. We do not explore the strategic questions latent in this scenario. These include whether it is in a state's interest to refrain from disclosure, maybe to avoid escalation but also to secretly exploit knowledge of the breach, or to remediate it quietly and avoid potentially damaging public controversy (Egloff 2020; Egloff and Smeets 2020). These are important issues, but our focus on state responses to public revelation merits separate treatment here.

To illuminate our five propositions, we provide narrative accounts of three illustrative cases from contemporary intelligence history that involve the United States. Each highlights key features of our argument. Edward Snowden allows us to explore the response of victim states like Germany to revelations about US digital espionage. We reflect upon how the

Snowden affair helped frame perceptions of digital espionage, particularly involving the US, and how this affects the way in which the other two cases were perceived. The compromise of the Office of Personnel Management, also during the Obama presidency, is a well-known example of Chinese digital espionage, a wider campaign of which led to indictments, sanctions, diplomacy and, in 2015, to a bilateral US-China agreement on certain forms of digital espionage. The third example, SolarWinds, provides the chance to evaluate the initial polarised public reception and its 'cost imposition' rhetoric, followed by the US government's more nuanced subsequent responses. We acknowledge that three case studies are limited in their international comparative potential and in the generalisability of our findings, particularly as the US – along with Russia and China – tends to dominate cybersecurity discourse and analysis in sometimes unhelpful ways. However, our narrow aim is to discern the extent to which states regard digital espionage as either exceptional or as comparable to other forms of espionage. If our propositions hold, we hope that further studies might build on them and explore other cases, particularly as our empirical understanding of cyber operations expands in scope and sophistication, and moves beyond the focus on US cyber competition with its adversaries to include a range of other examples (Valeriano and Maness 2018; Baig 2019; Ebert 2020; Shires 2021). It also allows us to offer some preliminary observations about how the US and like-minded nations can contribute to the development of stabilising norms for responding to digital political espionage.

1. Edward Snowden

Edward Snowden, a National Security Agency (NSA) contractor who in 2013 stole and leaked a massive trove of files about the activities of the agency and its allies, is different in several respects from the other cases in this article. Like the others, it involves the compromise of classified information on US networks, but the Snowden breach was a case of 'insider threat', not state-led espionage (Harding 2014). Moreover, although Snowden's activities necessarily entailed a breach of US intelligence networks and harmed US interests, the victim states were those targeted by US digital espionage, not the US itself. Snowden revealed an extensive global campaign of intelligence collection, which complicated bilateral relations between the US and several countries targeted by those campaigns (Harris 2014). As such, the Snowden case re-framed the strategic debate about digital espionage in the

context of public revelations about the scope, scale and techniques of US and wider Five Eyes intelligence practices.

The essential facts of Snowden's actions are widely reported (Harding 2014; Harris 2014). Whilst working as a low-level contractor to the NSA, Snowden became aware of and gradually disillusioned with a series of intelligence programmes he characterised as unconstitutional and amounting to mass surveillance of US citizens. Lacking confidence in the NSA's internal whistleblowing procedures and protection, over a period of about a year, Snowden copied unknown thousands of NSA documents onto portable storage media and smuggled them out of secure installations in Hawaii. In May 2013, Snowden tried to erase all digital traces of his life, travelled to Hong Kong to brief carefully selected journalists, and then to Moscow, where he eventually requested and was granted asylum. At the beginning of June 2013, *The Guardian* (UK) newspaper, followed by media outlets across the world, began publishing and reporting on selected documents from Snowden's archive. The breadth of espionage activities alleged by Snowden and his media and civil society partners was indeed extraordinary. Implicating intelligence agencies inside and outside the United States (notably, UK's GCHQ), and relying upon the alleged legal and operational complicity of major US technology companies, the NSA and its partners were, Snowden asserted, setting out 'to destroy privacy, internet freedom and basic liberties for people around the world with this massive surveillance machine they're secretly building' (Greenwald et al. 2013). In addition to capturing the personal digital interactions of millions of ordinary citizens in the name, principally, of US national security, the US was also accused of having spied on over 120 national leaders through digital and electronic means (Poitras et al. 2014). Whilst mindful of the problems of substantiating classified intelligence through non-classified means, and of extrapolating from what are often single data points, what Snowden revealed about the scale and scope of US digital espionage must rank as one of the most striking, if not necessarily the most consequential, exposures of the inner workings of intelligence of all time.

The precise nature of the activities of the NSA and its partners are not the focus of our attention here, nor are the motivations or morality of Edward Snowden. We also do not wish to consider further the reactions of the US government, which had to respond to the actions of an intelligence 'insider' disseminating information from within a federal

organisation to the public domain. Senior officials varied in their tone and estimates of damage, but all were united in their condemnation of Snowden's chosen mode of disclosure. The principal victims were those countries targeted by US digital espionage programmes. Many national leaders complained bitterly about the scale of US digital espionage and its demonstrable lack of regard for their national sovereignty and were appalled at the compromise of their own privacy, as well as that of their citizens. German Chancellor Merkel was said to be apoplectic that her personal telephone calls were intercepted by the NSA, likening the practice to the Stasi of her upbringing in East Germany (Traynor and Lewis 2013). Not unreasonably, she also called into question whether the NSA could be trusted to look after its own data, with which Snowden had absconded in apparently straightforward fashion. Brazilian President Dilma Rousseff was 'completely furious' about being personally targeted and demanded a public apology from the United States whilst also threatening to cancel an imminent state visit to Washington, DC (Winter 2013). In an extraordinary speech to the United Nations General Assembly a few weeks later, she identified US espionage activities as a breach of international law, drawing attention, like Merkel, to her own experiences with authoritarianism and surveillance (Borger 2013). In 2014, Brazil and the European Union announced plans for a new submarine cable between Latin America and Europe that would prevent data from the two regions being routed through the United States (Emmott 2014). This expressed a depth of feeling in the international community that was codified in a December 2013 UN General Assembly resolution denouncing digital surveillance and asserting digital privacy rights (United Nations 2013).

Notwithstanding these and other responses by states whose digital communications were intercepted by the NSA, tensions in their respective bilateral relationships with the United States were mostly short-lived. This was also the case for a country like Indonesia, whose targeting by Australia was revealed by Snowden, but who responded in frustrated yet restrained fashion, recognising the long-term importance of their strategic relationship (BBC 2013). This conforms with our opening propositions about the factors that determine the strategic consequences of digital espionage, namely that the circumstances of these revelations – such as otherwise friendly diplomatic relations – and the stark difference in relative power between surveilled states and the US, in particular, shaped the shorter,

milder repercussions of the incident. Longer-lasting effects were experienced by the US and its FVEY allies. The Snowden revelations forced a public re-evaluation of the ethics of FVEY intelligence collection policy (Walsh and Miller 2016). They also led to significant revision of legal 'bulk data' collection frameworks in the UK and elsewhere, updating legislation to keep pace with developments in digital surveillance (Bernal 2016). Without the Snowden leaks, it is unlikely these developments would have occurred in the same timeframe. Conversely, of course, whilst the Snowden revelations indelibly associated the United States with the growth of digital espionage, this period also saw digital espionage capabilities proliferate beyond such early-adopter states, including for example through the use of US contractors by the United Arab Emirates to improve its national capabilities (Bing and Schectman 2019). This added complexity (and urgency) to the challenge of understanding the strategic consequences of digital espionage, as more states have acquired these capabilities and explored the range of possible use cases in support of national strategy (Shires 2021).

2. Office of Personnel Management

The 2014 breach of the US Office of Personnel Management (OPM), leading to the loss of confidential data on US federal government employees, contractors, and their families and friends, was one of the largest ever reported breaches of US federal networks (Schmidt et al. 2014). Attributed to the Chinese government, it formed part of an extensive campaign of Chinese digital espionage, much of it focused on acquiring US intellectual property. As Adam Segal noted one year prior to the revelation of the OPM breach, a pattern had developed in which the US government wanted to roll back Chinese industrial espionage but was unwilling to accept any corresponding commitment to reduce US cyber espionage against Chinese targets (Segal 2013). Ultimately, the OPM breach led to the exfiltration of a large volume of data – reportedly nearly 22 million records – that could improve Chinese government understanding of the US federal workforce, potentially enabling tailored targeting of individuals for cultivation, extortion or other activities posing risks to their safety and security (Harknett and Smeets 2020, 21-23). The strategic significance of the breach was less immediately obvious. It is unclear, for example, whether (or to what extent) the OPM breach contributed to concerted US diplomatic pressure on the Chinese government, culminating in a 2015 bilateral China-US agreement to contain and curtail their respective espionage campaigns. This pledged that neither: 'will conduct or knowingly

support cyber-enabled theft of intellectual property, including trade secrets or other confidential business information for commercial advantage' (Nakashima and Mufson 2015). This agreement would not have covered the type of operation instantiated by the OPM breach, focusing as it did on commercial rather than political digital espionage. The US acknowledged a difference between the two types of espionage, with the then director of national intelligence, James Clapper, expressing a practitioner's begrudging respect that, 'You have to kind of salute the Chinese for what they did' (Groll 2015).

The impact of the recent Snowden case was plain from the beginning of the public controversy about the OPM breach. For example, the earliest *New York Times* report of the OPM breach referred directly to the complicating effect of Snowden's revelations – specifically US espionage against Huawei and Chinese political targets – on US efforts to broker a cyber espionage agreement with China (Schmidt et al. 2014). The same report noted that US strategy to constrain Chinese digital espionage – diplomatic negotiations, indictments of Chinese state hackers – was widely regarded as ineffective, quoting Obama's former Director of National Intelligence, who described the administration as 'speaking loudly and carrying a small stick'. In the year prior to the Obama-Xi agreement, the US government had indicted five Chinese military officials for digital espionage against commercial targets, the first ever such indictments of any foreign government officials (Nakashima and Wan 2014). It also signed an executive order authorising the imposition of economic sanctions against adversaries responsible for hostile cyber operations. According to an unnamed senior US government official quoted by the Washington Post on the signing of the Obama-Xi agreement, US diplomacy aimed 'to persuade the Chinese that this is not just something we are doing for domestic political consumption, but it is in fact a significant issue and a significant irritant in the bilateral relationship' (Nakashima and Mufson 2015).

Early analysis indicated that the 2015 agreement led to a reduction in Chinese commercial espionage against US targets, albeit such activity continued at a lower level and did not apply to political espionage like the OPM breach. The reduction was offset by increased digital espionage against other targets, such as firms in India, Japan and Taiwan (Menn 2015; Nakashima 2016). These reports also hinted that Chinese industrial espionage against US targets began to decrease a year before the Obama-Xi agreement, implying incremental success for the longer-term US strategy of increasing pressure through public indictments

and economic sanctions. As Adam Segal has argued, the US response to Chinese hacking is premised in their wider bilateral strategic relationship. Each has a national interest in preventing escalation and in developing norms of state behaviour in cyberspace through international cooperation; crucially, though, each will continue to pursue intelligence collection according to national strategic priorities (Segal 2013). This highlights the enduring tension between the strategic imperative to improve global cybersecurity and the parallel persistence of intelligence competition. In this context, the United States took several remedial steps following the OPM hack and other breaches but, consistent with our opening propositions, framed these as proportionate responses implemented to re-shape China's cyberspace conduct. This aligned with the US view that commercial espionage should be treated differently than the state-on-state espionage highlighted by the OPM breach, but without prejudice to the wider bilateral relationship.

3. SolarWinds

'SolarWinds' refers to a global digital espionage campaign, reportedly discovered in late 2020, that infected several thousand public- and private-sector organisations around the world and was actively used against a dozen or so US federal agencies and departments (Devanny 2021; Temple-Raston 2021). This was enabled by exploiting a supply-chain vulnerability in widely used IT administration software produced by the company SolarWinds (Bing 2020). The campaign was reportedly conducted by hackers associated with the Russian foreign intelligence service, the *Sluzhba Vneshney Razvedki* (SVR), also known as the advanced persistent threat (APT) actor APT29/'Cozy Bear' (Nakashima and Timberg 2020). The breach provoked a public debate about how the US government should respond and unfolded in the heat of the contested presidential transition between Presidents Trump and Biden. It was marked by persistent rhetoric about the need to 'impose costs' on Russia that underlined a tendency in public debate to conflate digital espionage with offensive cyber operations, with potentially dangerous implications for strategic stability (Martin 2021). The strategic consequences were further complicated by an intensifying global wave of ransomware attacks that prompted the US and other governments to consider further sanctions against Russia as an alleged 'safe harbour' for cyber-criminals. This matrix of interlocking dynamics provided the tense and uncomfortable strategic context in which the SolarWinds digital espionage campaign was revealed and responses to it were debated.

Domestically, the espionage campaign occurred during the final year of the Trump administration, but its revelation and ensuing discussion occurred immediately prior to Biden's inauguration and amidst Trump's challenge to the president-elect's legitimacy and the storming of the US Capitol in January 2021. The US response to SolarWinds was also complicated politically by the persistence of Russian espionage and manipulation as controversial tropes of the Trump administration. They were the central rationale for the Special Counsel investigation leading to the conviction of several Trump advisers and associates, which exacerbated Trump's distrust of and hostility towards the US intelligence community (Weissmann 2020). In this context, it is unsurprising that the Trump administration's immediate response to SolarWinds was slow and hampered by Trump's intervention on social media decrying efforts to attribute the breach to Russia (Devanny 2021, 17-19). In contrast, the Biden-Harris transition made an earlier, more conventional statement, framing its response in the form of a commitment to enhanced cybersecurity and, more problematically, in terms of willingness to impose costs following 'malicious cyber attacks' (Biden-Harris Transition 2020). Arguably, the transition team calculated that domestic politics required firm rhetoric about cost-imposition to differentiate Biden from Trump on issues relating to Russian intelligence operations.

The public debate about US responses to SolarWinds highlighted disagreements about how to categorise the breach: was it 'espionage as usual' or was it, as Microsoft's chief executive described it, 'effectively an attack on the United States and its government and other critical institutions, including security firms' (Smith 2020)? Some commentators connected the SolarWinds breach directly with a critique of US cyber strategy, arguing that an alternative, more restrained approach would better reduce cyber threats, and that any US response to SolarWinds should reflect the fact that the United States had conducted similar operations (Goldsmith 2020; Lin 2020). Conversely, prominent advocates of the post-2018 evolution in US cyber strategy assessed the breach as evidence confirming the need for persistent engagement in cyberspace (Harknett 2020). This discussion reflected a divergence of opinion between those who interpreted it as 'the arrival of digital apocalypse' and those who saw it as 'another major incident of cyber espionage' (Lawson and Valeriano 2020). The tenor of this debate was not assisted by a lack of technical understanding that allowed otherwise sensible US senators to frame SolarWinds as an 'act of war' (M. Miller 2020).

True to its initial response during the transition, in its first six months the Biden administration pursued a range of 'seen and unseen' responses to the SolarWinds breach and wider Russian state activities, including the poisoning of Russian opposition leader Alexei Navalny. The administration's decision to combine SolarWinds with a list of other Russian activities was an astute way to frame the US response more robustly than it would otherwise have to what was a relatively proportionate espionage operation. This extricated the administration from the expectations it had generated during the transition with its strong statements about cost-imposition. The elements of the US response included economic sanctions announced in April 2021, limited cyber operations targeting Russia's intelligence agencies and military, expulsions from the Russian diplomatic mission in Washington, DC, and a wider effort to stimulate more effective cybersecurity in the United States, initially through an executive order (Sanger et al. 2021). Biden's national security adviser, Jake Sullivan, publicly explained the rationale for using US cyber operations to signal US red lines and ultimately reshape adversary behaviour in cyberspace. At the same time, the Biden administration quickly revised the Trump era executive order on offensive cyber operations, retaining its improved latitude for lower-level operational autonomy but reasserting White House involvement in any operation with potentially escalatory consequences (Sanger et al. 2021).

The response to SolarWinds emerged as the administration also faced revelations about another major breach, this time of Microsoft, reportedly by Chinese state hackers, prompting broader questions about how the US should modulate its respective responses to Russian and Chinese cyber operations (Volz and Viswanatha 2021). In addition, in June 2021 the Biden administration joined other G7 governments in responding to another type of cyber threat, state-harboured rather than necessarily conducted by states, committing to improved international cooperation against ransomware (Sabbagh 2021). It is impossible at this early stage to judge the effectiveness of the Biden administration's initial responses to the SolarWinds breach. Given that the US response was framed as addressing a wider pattern of malign activity by the Russian government, it is unclear how the different elements are meant to be interpreted and what, if any, 'roadmap' exists to cultivating better bilateral relations. With both Russian and Chinese digital espionage, the problem of how to respond is complicated by the broader strategic context in which other issues – both

trade and security – are implicated. Similarly, it is difficult to credit Biden's description of the SolarWinds breach as 'totally inappropriate' and his administration's stated view that the US response aims to dissuade future such activity. This rings somewhat hollow, as the US has itself perpetrated significant and very long-running supply-chain operations (G. Miller 2020). The most plausible early assessment, consistent with our opening propositions, is that the Biden administration has adopted a conventional response, using a range of targeted economic sanctions, declaratory rhetoric, limited covert action, concerted diplomatic activity, and the old-fashioned expulsion of Russian officials from the Embassy. Cumulatively, this looks like a calculated effort to signal displeasure whilst also trying to contain the magnitude of the likely Russian counter-response within acceptable parameters.

Analysis

The three cases above highlight distinct features of state responses to cyber victimhood, and illustrate some of the domestic-political and geopolitical-strategic factors that shape those responses. In respect of our five initial propositions about how states are likely to respond to digital espionage, we can offer the following observations. In the wake of Snowden's revelations, most governments targeted by US digital espionage chose not to jeopardise bilateral relations with the United States or its Five Eyes partners. Countries like Brazil and Germany, initial performative outrage aside, recognised the strategic importance of their relations with the United States and chose not to imperil them through counterproductive escalation or provocation. Whether they would be unwise to defy a hegemon in any respect is moot, but they chose not to challenge the US over digital espionage, despite some sharp rhetoric for domestic and international consumption that served to distance themselves from specific US surveillance practices. This supports our opening propositions that lesser powers will tend to avoid provoking a greater power, and that friendly countries will be more lenient on one another than perhaps they would be to an adversary, whether great or small. In the years immediately following Snowden's revelations, the United States developed a diplomatic strategy to restrain Chinese industrial espionage and wider cyber espionage, of which the OPM breach represented one of the most significant compromises of federal networks. The Obama administration's response to the OPM breach and other instances of Chinese cyber espionage was essentially

proportionate and diplomatic, all within a strategic context that is less fraught with historical baggage than the US-Russia relationship.

In the short term, the Obama administration's response to the OPM breach and associated campaigns reduced the intensity of bilateral digital espionage, alerted both sides to the potentially escalatory aspects of digital espionage, and set an example to others that this problem could be managed given sufficient political will. This was despite prolonged domestic pressure – especially from lawmakers in Washington, DC – for precisely the types of countermeasures that might be deemed escalatory. The same applies in the case of the Biden administration's response to SolarWinds, which refused to adopt the hyperbole of some commentators, preferring a more measured and constructive response that avoided obvious escalation triggers. However, President-elect Biden did little to dampen the bellicose declarations of some in Congress, which may have forced his hand somewhat when in office.

It is striking that the United States publicly frames the SolarWinds breach (Russia) as 'totally unacceptable' and deserving of a range of consequences, all expressed in a more combative fashion than they have (to date) about the much less discriminate breach of Microsoft Exchange (China). The recklessness of the latter operation exposed its victims to wider risk of compromise, and yet the US response was modulated differently than towards the more carefully executed SolarWinds operation (Alperovitch and Ward 2021; Hudson and Nakashima 2021). Rather than the language and levers of coercive diplomacy used against Russia, Biden's response to Chinese digital espionage has so far followed a more restrained path: specific criminal indictments; efforts to improve cybersecurity; publication of a joint advisory detailing Chinese hackers' tactics, techniques and procedures; and coordinated diplomatic statements with US allies such as the other FVEY states, the European Union, NATO and Japan, criticising the irresponsibility of Chinese state behaviour in cyberspace (Ignatius 2021; Volz and Viswanatha 2021).

This indicates that strategic context matters when states consider their responses to high-profile victimhood. In this case, China is a near-peer competitor across a range of issues in a way that Russia is not. This supports our original proposition that peer competitors will respond proportionately and specifically to digital espionage campaigns: responses are

carefully calibrated because of the requirement to promote strategic stability. In the case of Microsoft Exchange, the US and China are both fully aware of their respective histories of digital espionage and the US has so far confined itself to the (by no means straightforward) task of pursuing coordinated attribution and diplomatic rebukes alongside likeminded states and organisations. These have their own strategic relationships with China in mind when framing their respective responses, hence differences in content and tone even in these coordinated statements (Borghard 2021a). Where SolarWinds is concerned, the US may feel able to respond more forcefully and punitively against a lesser power like Russia. In each case, however, the Obama and Biden administrations listened to but ultimately did not adopt the hawkish posture recommended by many domestic voices, although we should not forget that US cyber strategy writ large has become more expansive and proactive in doctrine and operations since 2018 (Devanny 2021; Healey 2019).

Whilst we acknowledge that three short case studies centred on a single country is not a suitable basis for generalisation, we find provisional support for our five initial propositions. First, that victim states respond proportionately and specifically to digital espionage, as they would do for HUMINT operations when exposed. Second, diplomatic and domestic political context have shaping effects on victim states' responses: domestic political considerations are weaker than might be expected and are almost always outweighed by strategic and geopolitical calculations, including the desirability of strategic stability; this puts national interest rather than political ideology *per se* at the heart of responses to digital espionage. Third, in situations of relative national power, we have seen that friendly states prefer clemency to escalation and, four, that less powerful states will avoid provocation and escalation. We may wonder what alternatives exist for most victims of a great power, but this again implies that national interests are best served by avoiding counter-productive conduct. On the other hand, as our fifth proposition articulates, a great power like the United States will treat a lesser power like Russia more firmly and punitively than it will a peer-competitor like China, albeit the responses to each have been carefully calibrated. Again, a small data set subject to qualitative investigation can only tell us so much; more work is required to substantiate these claims in a wider population of countries and cases.

In the case of Snowden, his revelations undoubtedly changed the global conversation about digital intelligence, with important implications for global governance and security, as well

as undermining US claims to moral superiority in respect of state behaviours in cyberspace. From that point forward, US assertions of irresponsible digital behaviour – by peers, in particular – would be met with accusations of hypocrisy and double standards, now conventional arguments in Chinese state media, for instance (e.g., Zhao 2021). It has also been key to counter-US moves in diplomatic fora. Accusations of US militarisation of cyberspace were a key factor in the UN Group of Governmental Experts on information security's failure to reach consensus in 2017 (Henriksen 2019), a process leading directly to a Russia-sponsored parallel diplomatic track in the UN General Assembly (Grigsby 2018). In addition to sensitising states and publics to the practices and possibilities of digital espionage, it has also legitimised those activities in the eyes of many: essentially, if the US can do it, why shouldn't others? This might not be the worst outcome, if we believe that espionage is a stabilising influence, but it might nonetheless complicate global regulation of a range of potentially destabilising activities. Interestingly, what little work has focused on the role of intelligence operations in shaping emerging norms of state behaviour argues that intelligence agencies have important roles to play as norm-setters in the international system. Specifically, they have 'converted cyberspace into a mere component of foreign intelligence operations' (Georgieva 2020: 48; also, Boeke and Broeders 2018). This has profound implications for global governance and the development and socialisation of a normative regime for cyberspace. In effect, states must learn not only how to respond to specific instances of digital espionage but also to the higher-level question, 'what is cyberspace for, if it is to be more than a playground for intelligence agencies?' Of course, it need not be any one thing at all, but squaring away competing interests has long been a central challenge for global cyber governance (Mueller 2010; Deibert 2013; Nye 2014; Powers and Jablonski 2015). The upshot of the norm-shaping agency of intelligence organisations is that it further highlights the crucial, parallel track of intelligence diplomacy that complements overt cyber diplomacy.

It is no coincidence that the decade of major, public cyber breaches explored in this article was also a period of significant innovation in government approaches to cybersecurity (Hannigan 2019). Whether the subject is the UK's inauguration of the National Cyber Security Centre in 2016, the US government's creation of the Cybersecurity and Infrastructure Security Agency in 2018, or the early post-SolarWinds efforts of the Biden

administration to improve cybersecurity, to name just three examples, the wider global history is of increasing salience of cyber as a national security priority, including in emerging powers that have developed cyber strategies and emergency response authorities over the past decade (Baig 2019; Ebert 2020; Sexton and Campbell 2020; Solar 2020). The increasing proficiency of US adversaries in this field – in part due to the loss of US equities – has intensified the problem and necessitated more emphasis on improving domestic resilience and achieving diplomatic outcomes with respect to norms of responsible state behaviour in cyberspace (Perlroth 2021). In contrast, Snowden is interesting for different reasons. Focusing on the wider strategic questions raised by Snowden, rather than the domestic US fallout, we have foregrounded two issues. First, the ways in which Snowden's revelations changed the global conversation about digital intelligence and shaped multilateral processes for promoting responsible state behaviour in cyberspace. Second, the issue of whether Snowden shifted the pace, scale or risk appetite of state actors responding to new knowledge of digital espionage. This is relevant to top-level strategic approaches to digital espionage highlighted by Snowden's revelations, or, for states already more-or-less aware of this prior to Snowden, in more granular and specific ways, emulating particular lines of access reported in the Snowden files or discovered subsequently. After Snowden, the Shadow Brokers leaks illustrated the potential for chaos and damage when intelligence agencies lose exploits developed to facilitate digital espionage (Loleski 2019; Perlroth 2021). Similarly, the cyber operations conducted against Qatar during the intra-GCC crisis from 2017 onwards – and subsequent apparent 'hack and leak' operation against the UAE – highlight the likelihood that, as digital capabilities proliferate, they will be used more aggressively – not simply for intelligence collection – by a range of states in pursuit of national strategic objectives (Jones 2017; Bing and Schectman 2019; Shires 2021).

Conclusion

At one level, the SolarWinds breach highlights how little has changed since Snowden in the mechanics of inter-state competition through digital espionage. The operation was sophisticated in execution and impressive in ambition, but it was not fundamentally different from other recent instances of digital espionage, or from the longer history of compromising supply-chains to generate intelligence, as in the case of Crypto AG (G. Miller 2020). This suggests that, despite the eruption of 'cyber Pearl Harbor' rhetoric demanding

severe cost imposition, an emerging body of experience exists for states to draw on in calibrating their responses to becoming victims of digital espionage, some of which is outlined here. Domestic political and prudential constraints might restrict the transparency of communication about these parameters. For example, no US government spokesperson (barring a character like Donald Trump, perhaps) is likely to respond to reporters with an indifferent shrug, avowing that the United States is an active participant in the global competition for advantage that is inter-state digital espionage. Public communication about a victim state's response is, therefore, at least a four-level game: (1) satisfying the domestic political audience, which is likely to feature a cohort advocating a stronger response than the administration intends; (2) assessing the impact of digital espionage on and within a specific bilateral relationship and its wider geopolitical significance. Two further international dimensions concern, respectively, adversary-facing and norm-shaping considerations: (3) shaping other adversary states' interpretations of how the victim state responds to such operations, emphasising 'red lines' and ultimately to deter future such operations (Borghard 2021b); and (4) reflecting on the universalizability of the response, addressing the global question about how the victim state wants its response to contribute to international normative debates about how states should respond to such operations. This reflective, norm-shaping aspect of decision-making for victim states is both prudential self-interest (Lieven 2021) – not wanting other states to respond similarly if the victim's own cyber operations are discovered – and motivated by concern for the wider strategic implications if other states were to emulate a response against their own digital adversaries.

The strategic consequences of digital espionage depend, therefore, to a large extent on the response of the victim state. As proposed initially, the specific context of bilateral relations between the victim state and the spying state will shape the chosen response. As with non-cyber issues, asymmetries of power constrain the range of options from which victim states feel able to choose. The state of broader diplomatic relations, and leader-to-leader relations, are relevant, but so too is the existence of an effective conduit for bilateral intelligence diplomacy. This is an important element in the effort to maintain equilibrium and to avoid cross-domain escalation. Effective digital intelligence diplomacy, running parallel to conventional cyber diplomacy, is therefore instrumental for the vitality and prospects of multilateral efforts to foster responsible state behaviour in cyberspace.

Securocrats, as well as diplomats, need to speak to each other about cyber issues. Where the current state of bilateral relations precludes such exchanges, there is perhaps scope for creative third parties to exercise convening power to help (re-)establish such channels. Biden's elevation of experienced cyber officials to senior national security roles is promising in this regard – an example to be emulated by other states – and illustrates the wider mainstreaming of cyber as a top national security issue (Ignatius 2021).

The cases examined above show that the United States has to date responded to cyber victimhood with restraint and a degree of self-awareness, notwithstanding increasing domestic pressure for stronger, more punitive responses. This is logical given the major power context of competition with Russia and China. Operational symmetry should guide proportionality of response: no US government would want a victim of US digital espionage to interpret that operation as an offensive act, with the 'cost imposition' implications that might entail. The underlying logic of this approach also accepts that digital espionage is not deterrable but is rather a persistent fact of international politics. As demonstrated by the Biden administration's response to SolarWinds, a prudent state response to cyber victimhood is to improve cybersecurity, both for the victim state and for other states and non-state actors, thereby increasing the cost of achieving success for adversaries.

The playbook of diplomatic responses should include continued focus on coordinated attribution diplomacy, and a campaign of indictments to impose specific reputational (state) and personal (indictee) costs commensurate with the significance of the associated operation. Finally, concerted bilateral and multilateral efforts should continue in order to constrain the most destructive and destabilising usage of offensive cyber capabilities, as well as sustained efforts to improve public understanding, so as to reduce domestic pressures for disproportionate retaliation to digital espionage. Just as cybersecurity is not cyber power, digital espionage does not equate to offensive cyber. Conceptual clarity can also improve governmental responses and, therefore, strategic stability. This raises a final, difficult issue about what states can and should say about their own digital espionage operations. Choices about this will determine the extent to which legislators and broader publics can ever appreciate precisely when an adversary's campaign has been symmetrical or has instead 'crossed a line.' These conversations will only proceed in an atmosphere of trust, trust that is not, after a decade of digital espionage revelations, in abundant supply.

Acknowledgements

The authors would like to thank the editors and reviewers for their constructive and helpful comments.

Disclosure statement

No potential conflicts of interest were reported by the authors.

Notes on contributors

Dr Joe Devanny is Lecturer in National Security Studies in the Department of War Studies, King's College London.

Professor Ciaran Martin CB is Professor of Practice in the Management of Public Organisations in the Blavatnik School of Government, University of Oxford.

Dr Tim Stevens is Senior Lecturer in Global Security in the Department of War Studies, King's College London.

ORCID

Joe Devanny: https://orcid.org/0000-0001-6031-2397

Ciaran Martin: https://orcid.org/0000-0001-8081-7712

Tim Stevens: https://orcid.org/0000-0001-6869-8810

References

Aitel, Dave, and Matt Tait. 2016. "Everything You Know About the Vulnerability Equities Process is Wrong'." *Lawfare*, August 18. Accessed 15 June 2021. https://www.lawfareblog.com/everything-you-know-about-vulnerability-equities-process-wrong.

Alperovitch, Dmitri and Ian Ward. 2021. "How Should the U.S. Respond to the SolarWinds and Microsoft Exchange Hacks?" *Lawfare*, March 12. Accessed 26 August 2021. https://www.lawfareblog.com/how-should-us-respond-solarwinds-and-microsoft-exchange-hacks.

Baig, Reda. 2019. “Could Offensive Cyber Capabilities Tip India and Pakistan to War?” *The Diplomat,* March 26. Accessed 26 August 2021. https://thediplomat.com/2019/03/could-offensive-cyber-capabilities-tip-india-and-pakistan-to-war/.

BBC. 2013. “Indonesia Leader Says Australia Spying Damaged Ties.” November 19. Accessed 24 June 2021. https://www.bbc.co.uk/news/world-asia-24986093.

Bernal, Paul. 2016. “Data Gathering, Surveillance and Human Rights: Recasting the Debate.” *Journal of Cyber Policy* 1(2): 243-264. doi: 10.1080/23738871.2016.1228990.

Biden-Harris Transition. 2020. “Statement by President-elect Joe Biden on Cybersecurity, 17 December.” Accessed 15 June 2021. https://buildbackbetter.gov/press-releases/statement-by-president-elect-joe-biden-on-cybersecurity/.

Bing, Christopher. 2020. “Hackers Spied on US Treasury Emails for a Foreign Government - Sources.” *Reuters*, December 13. Accessed 15 June 2021. https://uk.reuters.com/article/usa-cyber-treasury/exclusive-hackers-spied-on-u-s-treasury-emails-for-a-foreign-government-sources-idUSL1N2IT0KK.

Bing, Christopher and Joel Schectman. 2019. “Project Raven: Inside the UAE’s Secret Hacking Team of American Mercenaries.” *Reuters*, January 30. Accessed 25 August 2021. https://www.reuters.com/investigates/special-report/usa-spying-raven/.

Boeke, Sergei, and Dennis Broeders. 2018. “The Demilitarisation of Cyber Conflict.” *Survival* 60(6): 73-90. doi: 10.1080/00396338.2018.1542804.

Borger, Julian. 2013. “Brazilian President: US Surveillance a ‘Breach of International Law’.” *The Guardian*, September 24. Accessed 24 June 2021. https://www.theguardian.com/world/2013/sep/24/brazil-president-un-speech-nsa-surveillance.

Borghard, Erica. 2021a. “What Makes This Attribution of Chinese Hacking Different.” *Carnegie Endowment for International Peace*, July 22. Accessed 26 August 2021. https://carnegieendowment.org/2021/07/22/what-makes-this-attribution-of-chinese-hacking-different-pub-85023.

Borghard, Erica. 2021b. “Was SolarWinds a Different Type of Cyber Espionage?” *Lawfare*, March 9. Accessed 22 June 2021. https://www.lawfareblog.com/was-solarwinds-different-type-cyber-espionage.

Buchan, Russell. 2019. *Cyber Espionage and International Law*. Oxford: Hart Publishing.

Buchanan, Ben. 2018. *The Cybersecurity Dilemma: Hacking, Trust, and Fear between Nations.* London: Hurst & Company.

Cayford, Michelle, Wolter Pieters, and Constant Hijzen. 2018. “Plots, Murders, and Money: Oversight Bodies Evaluating the Effectiveness of Surveillance Technology.” *Intelligence and National Security* 33(7): 999-1021. doi: 10.1080/02684527.2018.1487159.

Daniel, Michael. 2014. “Heartbleed: Understanding When We Disclose Cyber Vulnerabilities.” *The White House*, April 28. Accessed 15 June 2021. https://obamawhitehouse.archives.gov/blog/2014/04/28/heartbleed-understanding-when-we-disclose-cyber-vulnerabilities.

Deibert, Ronald J. 2013. *Black Code: Inside the Battle for Cyberspace.* Toronto, ON: Signal.

Devanny, Joe. 2020. “The Ethics of Offensive Cyber Operations.” *Foreign Policy Centre*, December 3. Accessed 15 June 2021. https://fpc.org.uk/the-ethics-of-offensive-cyber-operations/.

Devanny, Joe. 2021. “‘Madman Theory’ or ‘Persistent Engagement’? The Coherence of US Cyber Strategy under Trump.” *Journal of Applied Security Research.* doi: 10.1080/19361610.2021.1872359.

Devanny, Joe, and Tim Stevens. 2021. “What Will Britain’s New Cyber Force Actually Do?” *War on the Rocks,* May 26. Accessed 17 June 2021. https://warontherocks.com/2021/05/what-will-britains-new-cyber-force-actually-do/.

Ebert, Hannes. 2020. “Hacked IT Superpower: How India Secures Its Cyberspace as a Rising Digital Democracy.” *India Review* 19 (4): 376-413. doi: 10.1080/14736489.2020.1797317.

Egloff, Florian J. 2020. “Public Attribution of Cyber Intrusions.” *Journal of Cybersecurity* 6(1): tyaa012. doi: 10.1093/cybsec/tyaa012.

Egloff, Florian J., and Max Smeets. 2021. “Publicly Attributing Cyber Attacks: A Framework.” *Journal of Strategic Studies*. doi: 10.1080/01402390.2021.1895117.

Emmott, Robin. 2014. “Brazil, Europe Plan Undersea Cable to Skirt US Spying.” *Reuters*, February 24. Accessed 24 June 2021. https://www.reuters.com/article/us-eu-brazil-idUSBREA1N0PL20140224.

Georgieva, Ilina. 2020. “The Unexpected Norm-Setters: Intelligence Agencies in Cyberspace.” *Contemporary Security Policy* 41(1): 33-54. doi: 10.1080/13523260.2019.1677389.

Gill, Peter. 2020. “Of Intelligence Oversight and the Challenge of Surveillance Corporatism.” *Intelligence and National Security* 35 (7): 970-989. doi: 10.1080/02684527.2020.1783875.

Gioe, David V. 2017. “‘The More Things Change’: HUMINT in the Cyber Age.” In *The Palgrave Handbook of Security, Risk and Intelligence*, edited by Rob Dover, Huw Dylan, and Michael S. Goodman, 213-227. Basingstoke: Palgrave Macmillan.

Gioe, David V., Michael S. Goodman, and Tim Stevens. 2020. “Intelligence in the Cyber Era: Evolution or Revolution?” *Political Science Quarterly* 135(2): 191-224. doi: 10.1002/polq.13031.

Goldsmith, Jack. 2020. “Quick Thoughts on the Russia Hack.” *Lawfare*, December 14. Accessed 15 June 2021. https://www.lawfareblog.com/quick-thoughts-russia-hack.

Government Communications Headquarters (GCHQ). 2018. “The Equities Process.” Accessed 15 June 2021. https://www.gchq.gov.uk/information/equities-process.

Greenwald, Glenn, Ewan MacAskill, and Laura Poitras. 2013. “Edward Snowden: The Whistleblower Behind the NSA Surveillance Revelations.” *The Guardian*, June 11. Accessed 15 June 2021. https://www.theguardian.com/world/2013/jun/09/edward-snowden-nsa-whistleblower-surveillance.

Grigsby, Alex. 2018. “The United Nations Doubles Its Workload on Cyber Norms, and Not Everyone Is Pleased.” Council on Foreign Relations, November 15. Accessed 21 June 2021. https://www.cfr.org/blog/united-nations-doubles-its-workload-cyber-norms-and-not-everyone-pleased.

Groll, Elias. 2015. “Clapper: ‘We Don’t Know Exactly What Was Taken in the OPM Breach’.” *Foreign Policy*, September 24. Accessed 24 June 2021. https://foreignpolicy.com/2015/09/24/clapper-we-dont-know-exactly-what-was-taken-in-the-opm-breach/.

Hannigan, Robert. 2019. “Organising a Government for Cyber: The Creation of the UK’s National Cyber Security Centre.” *Royal United Services Institute Occasional Paper*, February 27. Accessed 25 June 2021. https://static.rusi.org/20190227_hannigan_final_web.pdf.

Harding, Luke. 2014. *The Snowden Files: The Inside Story of the World's Most Wanted Man*. London: Guardian Faber Publishing.

Harknett, Richard J. 2020. “SolarWinds: The Need for Persistent Engagement.” *Lawfare*, December 23. Accessed 15 June 2021. https://www.lawfareblog.com/solarwinds-need-persistent-engagement.

Harknett, Richard J., and Max Smeets. 2020. “Cyber Campaigns and Strategic Outcomes.” *Journal of Strategic Studies.* doi: 10.1080/01402390.2020.1732354.

Harris, Shane. 2014. *@War: The Rise of the Military-Internet Complex*. New York: Houghton Mifflin Harcourt.

Healey, Jason. 2019. “The Implications of Persistent (and Permanent) Engagement in Cyberspace.” *Journal of Cybersecurity* 5(1): tyz008. doi: 10.1093/cybsec/tyz008.

Healey, Jason, and Robert Jervis. 2020. “The Escalation Inversion and Other Oddities of Situational Cyber Stability.” *Texas National Security Review* 3(4): 30-53. doi: 10.26153/tsw/10962.

Henriksen, Anders. 2019. “The End of the Road for the UN GGE Process: The Future Regulation of Cyberspace.” *Journal of Cybersecurity* 5(1): tyy009. doi: 10.1093/cybsec/tyy009.

Hitz, Frederick P. 2004. *The Great Game: The Myth and Reality of Espionage*. New York: Knopf.

Homburger, Zine. 2019. “The Necessity and Pitfall of Cybersecurity Capacity Building for Norm Development in Cyberspace.” *Global Society* 33(2): 224-242. doi: 10.1080/13600826.2019.1569502.

Hudson, John and Ellen Nakashima. 2021. “U.S., Allies Accuse China of Hacking Microsoft and Condoning Other Cyberattacks.” *Washington Post*, July 19. Accessed 26 August 2021., https://www.washingtonpost.com/national-security/microsoft-hack-china-biden-nato/2021/07/19/a90ac7b4-e827-11eb-84a2-d93bc0b50294_story.html.

Ignatius, David. 2021. “Opinion: An Undeclared War is Breaking Out in Cyberspace. The Biden Administration is Fighting Back.” *Washington Post*, August 10. Accessed 26 August 26, 2021. https://www.washingtonpost.com/opinions/2021/08/10/an-undeclared-war-is-breaking-out-cyberspace-biden-administration-is-fighting-back/.

Jervis, Robert. 2016. “Some Thoughts on Deterrence in the Cyber Era.” *Journal of Information Warfare* 15(2): 66–73.

Jones, Marc. 2017. “Hacking, Bots and Information Wars in the Qatar Spat.” *Washington Post*, June 7. Accessed 26 August 2021. https://www.washingtonpost.com/news/monkey-cage/wp/2017/06/07/hacking-bots-and-information-wars-in-the-qatar-spat/.

Lawson, Sean, and Brandon Valeriano. 2020. “The Russian ‘Cyber Pearl Harbor’ That Wasn’t.” Cato Institute, December 18. Accessed 25 June 2021. https://www.cato.org/publications/commentary/russian-cyber-pearl-harbor-that-wasnt.

Lefebvre, Stéphane, and Holly Porteous. 2011. “The Russian 10 … 11: An Inconsequential Adventure?” *International Journal of Intelligence & Counterintelligence* 24(3): 447-466. doi: 10.1080/08850607.2011.568290.

Libicki, Martin C., and Olesya Tkacheva. 2020. “Cyberspace Escalation: Ladders or Lattices?” in *Cyber Threats and NATO 2030: Horizon Scanning and Analysis*, edited by Amy Ertan, Kathryn Floyd, Piret Pernik, and Tim Stevens, 62-72. Tallinn: NATO Cooperative Cyber Defence Centre of Excellence.

Lieven, Anatol. 2021. “Biden’s Retaliatory Cyberattacks Against Russia are Folly.” *Responsible Statecraft*, March 11. Accessed 22 June 2021. https://responsiblestatecraft.org/2021/03/11/bidens-retaliatory-cyberattacks-against-russia-are-folly/.

Lin, Herb. 2020. “Reflections on the SolarWinds Breach.” *Lawfare*, December 22. Accessed 15 June 2021. http://www.lawfareblog.com/reflections-solarwinds-breach.

Loleski, Steven. 2019. “From Cold to Cyber Warriors: The Origins and Expansion of NSA’s Tailored Access Operations (TAO) to Shadow Brokers.” *Intelligence and National Security* 34(1): 112-128. doi: 10.1080/02684527.2018.1532627.

Lukoff, Lee. 2018. “Pardon Me? An Assessment of Jonathan Pollard’s Quest for Presidential Clemency.” *Journal of Intelligence History* 17(2): 85-103. doi: 10.1080/16161262.2018.1425032.

Martin, Ciaran. 2020. “Cyber Weapons are Called Viruses for a Reason: Statecraft, Security and Safety in the Digital Age.” King’s College London, November 10. Accessed 15 June 2021. https://thestrandgroup.kcl.ac.uk/event/ciaran-martin-cyber-weapons-are-called-viruses-for-a-reason-statecraft-security-and-safety-in-the-digital-age/.

Martin, Ciaran. 2021. “Cyber ‘Deterrence’: A Brexit Analogy.” *Lawfare*, January 15. Accessed 15 June 2021. https://www.lawfareblog.com/cyber-deterrence-brexit-analogy.

Menn, Joseph. 2015. “China Tried to Hack US Firms Even after Cyber Pact: CrowdStrike.” *Reuters*, October 20. Accessed 15 June 2021. https://www.reuters.com/article/us-usa-china-cybersecurity-idUSKCN0SD0AT20151020.

Miller, Greg. 2020. “The Intelligence Coup of the Century.” *Washington Post*, February 11. Accessed 15 June 2021. https://www.washingtonpost.com/graphics/2020/world/national-security/cia-crypto-encryption-machines-espionage/.

Miller, Maggie. 2020. “Lawmakers Ask Whether Massive Hack Amounted to Act of War.” *The Hill*, December 18. Accessed 24 June 2021. https://thehill.com/policy/cybersecurity/530784-lawmakers-ask-whether-massive-hack-amounted-to-act-of-war.

Mueller, Milton L. 2010. *Networks and States: The Global Politics of Internet Governance.* Cambridge, MA: The MIT Press.

Nakashima, Ellen. 2016. “Chinese Hacking Activity Down Sharply Since Mid-2014, Researchers Say.” *Washington Post*, June 20. Accessed 15 June 2021. https://www.washingtonpost.com/world/national-security/chinese-hacking-activity-down-sharply-since-mid-2014-researchers-say/2016/06/20/089703e6-36fd-11e6-9ccd-d6005beac8b3_story.html.

Nakashima, Ellen, and Steven Mufson. 2015. “US, China Vow Not to Engage in Economic Cyberespionage.” *Washington Post*, September 25. Accessed 15 June 2021. https://www.washingtonpost.com/national/us-china-vow-not-to-engage-in-economic-cyberespionage/2015/09/25/90e74b6a-63b9-11e5-8e9e-dce8a2a2a679_story.html.

Nakashima, Ellen, and Craig Timberg. 2020. “Russian Government Hackers are Behind a Broad Espionage Campaign that has Compromised US Agencies, Including Treasury and Commerce.” *Washington Post*, December 14. Accessed 15 June 2021. https://www.washingtonpost.com/national-security/russian-government-spies-are-behind-a-broad-hacking-campaign-that-has-breached-us-agencies-and-a-top-cyber-firm/2020/12/13/d5a53b88-3d7d-11eb-9453-fc36ba051781_story.html.

Nakashima, Ellen, and William Wan. 2014. "US Announces First Charges against Foreign Country in Connection with Cyberspying." *Washington Post*, May 19. Accessed 15 June 2021. https://www.washingtonpost.com/world/national-security/us-to-announce-first-criminal-charges-against-foreign-country-for-cyberspying/2014/05/19/586c9992-df45-11e3-810f-764fe508b82d_story.html.

Nye Jr., Joseph S. 2014. "The Regime Complex for Managing Global Cyber Activities." *Global Commission on Internet Governance Paper Series* 1. Accessed 21 June 2021. https://www.cigionline.org/sites/default/files/gcig_paper_no1.pdf.

Omand, David. 2015. "Understanding Digital Intelligence and the Norms That Might Govern It." *Global Commission on Internet Governance* 8, March. Accessed 25 August 2021. https://www.cigionline.org/sites/default/files/gcig_paper_no8.pdf.

Omand, David, and Mark Phythian. 2018. *Principled Spying: The Ethics of Secret Intelligence.* Oxford: Oxford University Press.

Pawlak, Patryk, and Panagiota-Nayia Barmpaliou. 2017. "Politics of Cybersecurity Capacity Building: Conundrum and Opportunity." *Journal of Cyber Policy* 2(1): 123-144. doi: 10.1080/23738871.2017.1294610.

Pepper, David. 2010. "The Business of SIGINT: The Role of Modern Management in the Transformation of GCHQ." *Public Policy and Administration* 25(1): 85-97. doi: 10.1177/0952076709347080.

Perlroth, Nicole. 2021. *This is How They Tell Me the World Ends: The Cyber Weapons Arms Race*. London: Bloomsbury.

Poitras, Laura, Marcel Rosenbach, and Holger Stark. 2014. "GCHQ and NSA Targeted Private German Companies and Merkel." *Der Spiegel*, March 29. Accessed 15 June 2021. https://www.spiegel.de/international/germany/gchq-and-nsa-targeted-private-german-companies-a-961444.html.

Powers, Shawn M., and Michael Jablonski. 2015. *The Real Cyber War: The Political Economy of Internet Freedom.* Urbana, IL: University of Illinois Press.

Putnam, Robert. 1988. “Diplomacy and Domestic Politics: The Logic of Two-Level Games.” *International Organization* 42 (3): 427-460. doi: 10.1017/S0020818300027697.

Resnyansky, Lucy. 2010. “The Role of Technology in Intelligence Practice: Linking the Developer and the User Perspectives.” *Prometheus* 28 (4): 361-374. doi: 10.1080/08109028.2010.544076.

Sabbagh, Dan. 2021. “Ransomware is Biggest Online Threat to People in UK, Spy Agency Chief to Warn.” *The Guardian*, June 14. Accessed 15 June 2021. https://www.theguardian.com/technology/2021/jun/14/ransomware-is-biggest-online-threat-to-people-in-uk-spy-agency-chief-to-warn.

Sanger, David E., Julian E. Barnes, and Nicole Perlroth. 2021. “Preparing for Retaliation Against Russia, US Confronts Hacking by China.” *New York Times*, March 7. Accessed 15 June. https://www.nytimes.com/2021/03/07/us/politics/microsoft-solarwinds-hack-russia-china.html.

Schia, Niels N., and Lars Gjesvik. 2020. “Hacking Democracy: Managing Influence Campaigns and Disinformation in the Digital Age.” *Journal of Cyber Policy* 5 (3): 413-428. doi: 10.1080/23738871.2020.1820060.

Schmidt, Michael S., David E. Sanger, and Nicole Perlroth. 2014. “Chinese Hackers Pursue Key Data on US Workers.” *New York Times*, June 7. Accessed 15 June 2021. https://www.nytimes.com/2014/07/10/world/asia/chinese-hackers-pursue-key-data-on-us-workers.html.

Scott, Len. 2013. “Human Intelligence.” In *Routledge Companion to Intelligence Studies*, edited by Robert Dover, Michael S. Goodman, and Claudia Hillebrand, 96-104. London: Routledge.

Segal, Adam. 2013. “The Code Not Taken: China, the United States, and the Future of Cyber Espionage.” *Bulletin of the Atomic Scientists* 69 (5): 38-45. doi: 10.1177/0096340213501344.

Sexton, Michael and Eliza Campbell (eds.). 2020. *Cyber War and Cyber Peace in the Middle East: Digital Conflict in the Cradle of Civilization.* Washington, D.C.: The Middle East Institute.

Shires, James. 2021. “The Cyber Operation Against Qatar News Agency.” In Mahjoob Zweiri, Md Mizanur Rahman and Arwa Kamal (eds.). *The 2017 Gulf Crisis: An Interdisciplinary Approach*. Singapore: Springer, 101-113.

Smith, Brad. 2020. “A Moment of Reckoning: The Need for a Strong and Global Cybersecurity Response.” *Microsoft*, December 17. Accessed 15 June 2021. https://blogs.microsoft.com/on-the-issues/2020/12/17/cyberattacks-cybersecurity-solarwinds-fireeye/.

Solar, Carlos. 2020. “Cybersecurity and Cyber Defence in the Emerging Democracies.” *Journal of Cyber Policy* 5 (3): 392-412. doi: 10.1080/23738871.2020.1820546.

Temple-Raston, Dina. 2021. “A 'Worst Nightmare' Cyberattack: The Untold Story of the SolarWinds Hack.” *National Public Radio*, April 16. Accessed 15 June 2021. https://www.npr.org/2021/04/16/985439655/a-worst-nightmare-cyberattack-the-untold-story-of-the-solarwinds-hack.

Traynor, Ian, and Paul Lewis. 2013. “Merkel Compared NSA to Stasi in Heated Encounter with Obama.” *The Guardian*, December 17. Accessed 15 June 2021. https://www.theguardian.com/world/2013/dec/17/merkel-compares-nsa-stasi-obama.

United Nations. 2013. “General Assembly Backs Right to Privacy in Digital Age.” December 19. Accessed 24 June 2021. https://news.un.org/en/story/2013/12/458232-general-assembly-backs-right-privacy-digital-age.

United Nations Group of Government Experts (UN GGE). 2021. “Advance Copy: Report of the Group of Governmental Experts on Advancing Responsible State Behaviour in Cyberspace in the Context of International Security.” May 28. Accessed 15 June 2021. https://front.un-arm.org/wp-content/uploads/2021/06/final-report-2019-2021-gge-1-advance-copy.pdf.

Urban, Mark. 2018. *The Skripal Files: The Life and Near Death of a Russian Spy*. London: Macmillan.

Valeriano, Brandon, and Ryan C. Maness. 2018. "How We Stopped Worrying about Cyber Doom and Started Collecting Data." *Politics and Governance* 6 (2): 49-60. doi: 10.17645/pag.v6i2.1368.

Volz, Dustin and Aruna Viswanatha. 2021. "Biden Administration Blames Hackers Tied to China for Microsoft Cyberattack Spree." *Wall Street Journal*, July 19. Accessed August 26, https://www.wsj.com/articles/biden-administration-to-blame-hackers-tied-to-china-for-microsoft-cyberattack-spree-11626692401.

Walsh, Patrick F., and Seumas Miller. 2016. "Rethinking 'Five Eyes' Security Intelligence Collection Policies and Practice Post Snowden." *Intelligence and National Security* 31(3): 345-368. doi: 10.1080/02684527.2014.998436.

Warner, Michael. 2017. "Intelligence in Cyber – and Cyber in Intelligence." In *Understanding Cyber Conflict: Fourteen Analogies*, edited by George Perkovich, and Ariel E. Levite, 17-29. Washington, DC: Georgetown University Press.

Weissmann, Andrew. 2020. *Where Law Ends: Inside the Mueller Investigation*. New York: Random House.

Whyte, Christopher. 2020. "Beyond Tit-for-Tat in Cyberspace: Political Warfare and Lateral Sources of Escalation Online." *European Journal of International Security* 5(2): 195-214. doi:10.1017/eis.2020.2.

Wight, Martin. 1977. *Systems of States.* Leicester: Leicester University Press.

Winter, Brian. 2013. "Brazil's Rousseff Wants US Apology for NSA Spying." Reuters, September 4. Accessed 24 June 2021. https://www.reuters.com/article/us-usa-security-snowden-brazil-idUSBRE98314N20130904.

Wolf, Markus. 1997. *Without a Face: The Autobiography of Communism's Greatest Spymaster.* New York: Random House.

Zhao, Manfeng. 2021. “The Big Brother is Watching You!” *China Daily*, June 2. Accessed 21 June 2021. http://global.chinadaily.com.cn/a/202106/02/WS60b70b2da31024ad0bac315c.html.