<a>11. Civil Society in Cyberwarfare: Hack-and-Leaks, Attribution and Mobilisation

James Shires

<b>Introduction

This chapter explores the role of civil society in cyberwarfare. Following an opening section defining the term, it then examines why civil society and cyberwarfare are not usually considered natural conceptual companions: unlike cyberwarfare, civil society is fundamentally neither covert nor designed to further state interests. Nonetheless, civil society has participated extensively in shaping international rules and norms for cyberwarfare, addressed in the subsequent sections. The second half of the chapter identifies four underappreciated ways in which civil society has influenced cyberwarfare: in its popular cultural origins and reference points; through the development of the tactic of hack-and-leak operations; by attributing and revealing key cyberwarfare actors and campaigns; and through popular mobilisation. The chapter concludes with a personal reflection on the role of civil society in research and analysis on cyberwarfare.

<b>Defining civil society

Civil society, broadly speaking, is best defined negatively: it is any institution that is neither within the traditional branches of government (legislative, executive, judiciary), nor a for-profit producer of goods or services. While early economic theory conceived of profit-making companies (public or private) as a core part of civil society, modern usage now treats markets as a separate sphere. Civil society thus primarily denotes formally defined and institutionalised non-governmental organisations (NGOs), charities, political parties, unions, professional associations, and other non-profit entities.

Civil society includes the more amorphous category of ‘social movements’, encompassing many other kinds of voluntary groups, either with explicitly political or other purposes (Porta

and Tarrow, 2004). Civil society also includes individuals, whose actions – coming together organically or with cumulative impact separately – do not always occur under a formal umbrella. In cyberwarfare, this kind of activity is most often described as ‘hacktivism’ - a portmanteau of ‘hacking’ and ‘activism’ - with key cases analysed in more detail in the following sections (Coleman, 2014).

Politically, civil society is a central aspect of democratic governance. Civil society facilitates public deliberation of political issues, as well as the development of interest and advocacy groups to influence policy, government and business decisions (Diamond, 1994). The bounds of civil society, and consequently the boundaries of its permissible political influence, are regulated by states in very different ways. In more authoritarian settings, groups like professional associations and unions are often banned (Bishara, 2018). Even in less authoritarian contexts, protests, direct action, and other forms of activism tread a fine line between attracting attention and inviting legal sanction.

The interaction of civil society with government bodies and companies also deserves scrutiny, as the possibilities afforded to civil society organisations can lead to their exploitation and co-option by other entities (Burchell and Cook, 2013). In cyberwarfare, this is most often known as proxy action, examined in a previous chapter of this handbook (Schmoldt, this volume). As noted there and discussed later in this chapter, the definition and identification of a state proxy, as opposed to a genuine civil society actor, can be very challenging.

Two societal sectors are key parts of civil society, although not necessarily meeting the criteria of a non-profit entity. First, a free and open media is central to democratic governance, and media organisations often perform civil society functions of holding government and businesses to account, as well as influencing popular and elite attitudes to government – and of course, actual votes (Habermas, 2006). This ideal is rarely realised in

practice, with many countries exhibiting a polarised, for-profit media sector and/or a predilection for censorship and repression (Lavie and Yefet, 2022). Insofar as cyberwarfare includes information operations as well as more technical intrusion or interference with digital systems and networks, media organisations are both a key vector and means of countering such operations. The rise of social media companies as primary platforms for political debate – although not technically part of civil society themselves - means that their profit incentives and regulatory structure have reshaped the landscape of information and disinformation (Gorwa, 2019).

Second, academic institutions are traditional defenders of free speech and independent research and analysis, in addition to their vital educational role in society. The values of objectivity and scientific integrity in academic institutions are well-entrenched, although they have faced significant challenges in the digital age (Eringfeld, 2021). With regards to cyberwarfare, academic institutions have been entangled in information operations and disinformation (FireEye Intelligence, 2018), although – as later sections demonstrate – ideas of academic objectivity and, crucially, legal structures of independence and free speech in universities, have been central to their ability to attribute cyberwarfare operations (Deibert, 2020).

<b>Civil society and cyberwarfare

If we understand cyberwarfare as predominantly a practice of military and intelligence agencies (Chesney and Smeets, 2023), and its purpose – like warfare more generally – as being to advance the interests of states and achieve their strategic objectives (Gioe et al., 2020; Harknett and Smeets, 2022), then understanding the role of civil society in cyberwarfare seems to pose a problem on both fronts. First, civil society is not only located well outside the highly classified worlds of military and intelligence but in many cases is diametrically opposed to it. NGOs like Privacy International and Big Brother Watch in the

UK, and the Electronic Frontier Foundation (EFF) and the American Civil Liberties Union (ACLU) in the US, have focused much of their research and advocacy against the curtailment of individual rights of freedom of expression and privacy, especially around government adoption of digital technologies. For such organisations, military and intelligence cyber operations are one part of a broader phenomenon of state overreach, wherein such agencies are permitted overly broad powers for the collection, analysis, and use of digital signals intelligence (SIGINT) under the rubric of counterterrorism or other national security justifications (Gellman, 2021).

The paradigmatic cases of Wikileaks' 'Public Library of US Diplomacy', leaked by Chelsea Manning in 2010, and the National Security Agency (NSA) leaks by Edward Snowden in 2014, illustrate the depth of opposition between civil society and cyberwarfare organisations. In both cases, a civil society actor released massive amounts of government classified information, with a claimed moral motivation of defeating excessive state secrecy and exposing privacy and other human rights violations (Bauman et al., 2014). In both cases, the individuals involved were subject to criminal prosecution in the US for espionage, with Manning released after four years, Wikileaks founder Julian Assange pending extradition from the UK, and Snowden in exile in Russia. These cases pitted civil liberties organisations against Western intelligence agencies and governments, leading to bitter disputes in courts, parliaments and the media (Lyon, 2015). They also shifted public opinion and civil society campaigning beyond the states of the Five Eyes intelligence alliance (the US, UK, Canada, Australia, and New Zealand), as states and civil society around the word reread US promotion of internet freedom and human rights in light of a long history of similar surveillance as highly hypocritical (Mainwaring and Aldrich, 2019). Many parts of civil society, then, appear not only not to participate in cyberwarfare, but are fundamentally opposed to its practice and conduct on human rights grounds.

The second problem in relating civil society to cyberwarfare is the purpose of cyberwarfare to further state interests (Devanny et al., 2021). Civil society, in contrast, is fundamentally transnational. Civil society organisations routinely have close affinities, share values, and work together with their counterparts in other countries. Indeed, a classic work on the impact of civil society movements sees their transnational connections as central to their ability to generate new international norms (Keck and Sikkink, 1998). However, their transnational character makes them the target of government suspicion in some states, where 'foreign funding' for NGOs is a red flag or even a reason for state-imposed closure. Overall, transnational civil society is not only opposed to cyberwarfare for human rights reasons around its conduct, but equally due to its role in statecraft and interstate geopolitical struggles.

These two tensions mean that the best starting point for analysing civil society and cyberwarfare is in the development of legal and normative constraints to cyberwarfare: its rules and norms.

<b>Civil society contribution to rules and norms for cyberwarfare

The uncertain status of rules and norms on cyberwarfare at the United Nations (UN) and other multilateral forums means that civil society has the opportunity – if not always the platform – to influence such norms. While the final section of this handbook addresses cyberwarfare governance in more detail, any discussion of the role of civil society must highlight three points about its role in this arena.

First, cybersecurity and internet governance – two issues intimately related to cyberwarfare - have historically been exemplars of 'multistakeholder' governance, in which states, companies and civil society all contribute to decision-making and agenda-setting (Raymond and DeNardis, 2015). Multistakeholder governance does not necessarily imply equality, and

civil society participants are not always given equal weight even in technical meetings of non-profit organisations that operate key internet infrastructure (Jongen and Scholte, 2022). Furthermore, many members of these organisations struggle to reconcile their highly technocratic discussions with the kinds of value-based advocacy and campaigning traditionally associated with civil society. Indeed, this has been a key source of tension in such settings, as activist groups have used supposedly technical document formats and meetings to raise value-driven concerns (ten Oever, 2019). Similarly, the convoluted formality of decision-making at such technocratic bodies has exposed the fragility of internet governance, especially at moments of high pressure (Campbell and Gahnberg, 2022).

Second, UN processes have become increasingly open to the inclusion of civil society representatives. The first UN process on cybersecurity, a Group of Governmental Experts (GGE), included representatives from a handful of select states. Its successors, the two iterations of the Open-Ended Working Group (OEWG), included civil society participants far more centrally, with briefings before and after the main negotiation sessions, as well as many side events (Kumar, 2021). However, civil society participants remained unable to contribute during the main sessions, and more recently – given the location of the OEWG in New York – civil society participation has been restricted due to principled visa refusal by Ukraine and, in response, Russia (Johnson, 2022).

Other recent UN processes, such as the Ad Hoc Committee on Cybercrime (AHC), have included greater civil society representation, with allotted space for multistakeholder interventions during each negotiating session, and dedicated intersessional meetings (Hakmeh and Pawlak, 2021). While the remit of the AHC is not cyberwarfare – indeed, the current draft of the treaty text emphasizes its focus only on countering criminal cyber threats – its discussions of international cooperation and capacity-building cover very similar ground to

some of the norms agreed in the processes directly addressing state behaviour (see Baram and Peer, this volume).

Third, recent years have seen the development of multistakeholder governance processes that are neither more technically focused internet governance nor formal UN negotiations. Initiatives such as the Paris Call and the Cyber Tech Accord bring states, private sector, and civil society together to discuss rules and norms (Ruhl *et al.*, 2020). Indeed, some civil society institutions emerging from this moment, like the CyberPeace Initiative, highlight their opposition to cyberwarfare in their name. The CyberPeace Initiative has funding from charitable foundations and major tech companies – especially Microsoft – which also sponsors multistakeholder forums like the European Cyber Agora, now in its third year. While scholars have raised questions about Microsoft's specific role in the cyber norms landscape (Hurel and Lobato, 2018; Liebetrau and Monsees, 2023), the key point here is that civil society influences conversations about cyberwarfare rules and norms both directly – in the substance of those discussions themselves – and more indirectly.

A good example of civil society contributions to norms on cyberwarfare is in understanding cyberwarfare as a gendered issue – i.e., one to which people of different genders contribute in different ways, and the impact of which affects people of different genders unequally (Millar et al., 2021). Civil society and academia have long argued for greater consideration of the gendered impacts of cybersecurity more broadly, but these debates had largely set aside the interstate interactions that are the substance of cyberwarfare. This is beginning to change. International NGOs have written influential papers explaining how gender matters for international, as well as interpersonal, cybersecurity (Brown and Pytlak, 2020), while others have studied the gendered elements of information operations (Judson et al., 2020). Some, such as the Centre for Feminist Foreign Policy, have demonstrated how a feminist perspective on the militarization of cyberspace – and, in contrast, feminist cyber peace – are crucial to

understanding and preventing cyberwarfare (Bernarding and Kobel, 2023). Finally, such work also advocates for an intersectional gender perspective on cyberwarfare, illuminating how aspects of identity including race, class, sexual orientation, age and ability intersect with gender to determine the impacts of cyber operations on particular individuals and groups (de Oliveira and Slupska, 2023).

Building on the role of civil society in contributing to rules and norms for cyberwarfare, the following section examines four ways in which civil society has influenced cyberwarfare: through popular culture, hack-and-leak tactics, innovations in attribution, and popular mobilisation.

<b>Civil society, popular culture and the origins of cyberwarfare

As noted above, the media sector is an essential element of civil society. Media depictions of cyberwarfare in factual programming such as news and analysis are highly influenced by popular culture, as writers and producers seek clear reference points to help their audience understand complex topics. Consequently, representations of cyberwarfare in popular culture (primarily in visual arts such as film and television) are a crucial backdrop to all public discussions of cyberwarfare, including those involving civil society actors like NGOs and hacktivists considered below (Dunn Cavelty, 2019).

Early hackers were highly cognizant of their representation and image, as well as their actions. Indeed, legendary hacker groups like the Cult of the Dead Cow went to great lengths to cultivate and develop the trope of the geeky, mischievous but well-intentioned misfit that is – sometimes - still associated with hacking today (Menn, 2020). For such groups, their hacking activities were one part of a broader countercultural agenda, epitomised by their interaction with publications like Steward Brand's *Whole Earth Catalog*. Some Cult of the Dead Cow members eventually advised mainstream cyberwarfare actors in government and

the private sector – most notably, Peiter Zatko, aka Mudge, ran several influential projects at the Defense Advanced Research Projects Agency (DARPA) from 2010-2013 – thereby transmitting their understanding of cyberwarfare directly to relevant actors.

The origins of cyberwarfare in popular culture also precede its origins in fact. Early skirmishes in cyberwarfare are usually cited as the US 1997 exercise Eligible Receiver (in which cyber operators swiftly 'owned' their designated opponents' systems), or the 1999 'Moonlight Maze' intrusion (in which Russian intruders were identified in US Department of Defense (DoD) networks), or even the 1986 KGB intrusion recounted in Clifford Stoll's book *The Cuckoo's Egg* (Stoll, 2005; Healey, 2013; Raiu *et al.*, 2017). However, cyberwarfare in popular culture began even earlier, with the 1983 film *War Games*, in which a teenage hacker almost precipitated nuclear war. *War Games* was famously screened by US President Ronald Reagan in the White House shortly after its release, causing Reagan to consider the genuine feasibility of the on-screen scenario and create a taskforce to investigate the potential for cyberwarfare between the US and the Soviet Union (Poetranto, 2019).

Although not at the same level of existential risk, subsequent US conflicts were abound with instances of supposed cyberwarfare drawing on the *War Games* trope. Operation *Desert Storm* in the 1990–1 Gulf War spawned claims of highly successful electronic warfare, spurious stories about viruses smuggled into Iraqi command centres, and genuine Dutch hackers seeking to offer information about the US military to the Iraqi government (Shires, 2021, p. 77). Iraq's centrality for the US national security establishment meant that a few years later, in 1998, a series of document thefts from the US military over internet networks was initially suspected to be the work of Iraqi government hackers. The culprits later turned out to be teenage hackers in the US and Israel (Shires, 2021a).

More generally, I have argued elsewhere that the popular impression of cyberwarfare as 'cyber-noir' – 'a gloomy underworld in which the good guys must resort to unconventional

tactics to keep at bay a motley group of threats to the digital safety of unsuspecting individuals, businesses, and governments' – is crucial in shaping the self-impression and conduct of cybersecurity and cyberwarfare practitioners (Shires, 2020, p. 82). Consequently, we should examine some claims of cyberwarfare, as I argue in that piece, 'not straight-faced, as signs of impending doom, but less seriously as ironic nods to wider popular culture' (Shires, 2020, p. 101). Civil society, in the broadest sense, is both the origin of and counterweight to the more extreme hype around cyberwarfare in government and expert circles. The next section shows how civil society also influences cyberwarfare at the more detailed level of tactical and technical development, rather than in framing and representation.

<b>Civil society tactics of cyberwarfare: hacking and leaking

One prevalent tactic in cyberwarfare is hack-and-leak operations. Originally, hack-and-leaks were mainly conducted by civil society actors or individual hackers, also known as 'doxing'. Doxing — the acquisition and publication of another individual's private information — is one of the oldest practices in cyberspace. Originally, to 'dox' (from 'documents') someone meant simply revealing their offline identity, either 'for the lulz' — for little discernible reason beyond personal enjoyment — or to embarrass those who transgressed early norms of behaviour on the internet (Shires, 2020b).

As the internet grew, doxing became more sophisticated, using both intensive open-source investigation and intrusion into the target's systems to obtain sensitive information. The targets changed too, from tit-for-tat spats within hacker communities to the publication of personally identifiable information for thousands of government and corporate employees. These later events are 'public-interest hacks,' in Gabriella Coleman's description of the hacker collective Anonymous, or what Bruce Schneier has called 'political' or 'organizational' doxing (Coleman, 2014; Schneier, 2015). Notorious hack-and-leaks with

apparently moral motivations have also targeted the cyberwarfare industry itself, with a hacker named 'Phineas Fisher' claiming hack-and-leak operations that released many internal documents of spyware companies (on which more in the following section) (Shires, 2021, pp.132-140). Others – for example, the 'Football Leaks' exposing the financial scandals of major European football teams – are even more clearly cases of individuals finding new ways to expose what they see as morally and legally corrupt practices (Knight, 2019).

While some observers have suggested Phineas Fisher is an alias for a state-sponsored actor, the jury remains out (Menn, 2020). Other incidents – while also murky – have more concrete, if circumstantial, proof behind them. One case I have investigated in previous research is that of the so-called Yemen Cyber Army, who in 2015 released thousands of documents from the Saudi Arabian Ministry of Foreign Affairs (Shires, 2019). Technical clues point to a compromise of the Saudi embassy in Ukraine by Russian state cyber actors, and use of infrastructure closely linked to the same group. Analysts recognize that Iranian sponsorship would also be a logical conclusion, given the long history of companies and 'hacktivist groups' conducting cyber operations for the Iranian state (Rid, 2020; Shires and McGetrick, 2021). Further examination of such links is beyond the scope of this chapter, taking us away from civil society and more firmly into the territory of state proxies (Schmoldt, this volume).

Even if these specific cases remain uncertain, the broader trend is obvious. As some observers noted after the paradigm-shifting hack-and-leak of the Democratic National Committee (DNC) during the US Presidential election campaign in 2016, the trajectory of hack-and-leaks went as follows: 'it used to be teens, then criminals, then nation-states, and now it's nation-states pretending to be teens' (Kelty and Coleman, 2017). As well as the DNC leaks, notable state-sponsored hack-and-leak operations have taken place against international sporting bodies (the World Anti-Doping Agency, WADA), private entities in the US (Sony

Pictures), and in other national contexts (Macronleaks, the 2019 UK election, and the Saudi cables), as well as in many more situations of destabilisation and conflict (Shires, 2021b).

The rise of ransomware as a top-tier national security threat in many countries has led to close attention on the potential for such operations to indirectly leak sensitive information. Cybersecurity industry reports have, for example, highlighted the related strategic pay-offs for leaking and blackmail in Iranian ransomware operations in Israel (Lomashvili, 2022). In Ukraine, Russian groups – some acting as state proxies, others as part of a criminal ecosystem that I distinguish sharply from civil society – have also used ransomware operations for both disruption and exposure (Burgess, 2022).

Overall, state hack-and-leak operations are now highly complex. Understanding the multiple levels of influence in each case means unpacking their specific means of access and dissemination, and the associated possibilities for falsification and contestation (Shires, 2021b). Hack-and-leak operations are now part of the standard repertoire of digital disinformation operations conducted by intelligence agencies, combining intrusion into networks with coordinated and doctored dissemination through traditional and social media. However, while hack-and-leak operations fit into a long history of the manipulation of information for national security purposes, which is centrally the preserve and currency of intelligence agencies, the tactic was originally developed and refined by civil society.

<b>Civil society and cyberwarfare attribution

A separate cyberwarfare function played by civil society is that of attribution: identifying the perpetrator of a cyberattack at the technical, individual, organisational, or state level. The ‘attribution question’ that arises after a cyberattack is a process of meaning-making, shorthand for a very complex series of investigative inferences and assessments (Egloff and Dunn Cavelty, 2021). Cyberattacks do not speak for themselves, especially when states do

not avow them, and so public attribution is fundamentally a political and technological process, with many possible readings at the same time.

In particular, Citizen Lab, an interdisciplinary organisation based at the University of Toronto, has played an integral role in cyberwarfare attribution. Citizen Lab was formed in 2009, and the director of Citizen Lab, Ron Deibert, has explicitly stated that his aim is to promote an alternative 'human security' version of cybersecurity that puts the security of individuals and communities before national or other security priorities (Deibert, 2018, 2020). Citizen Lab leveraged a powerful genre established around private-sector attribution of state cyber operations —which they, incidentally, helped to start—repurposing its discursive characteristics to attribute spyware used by states against journalists, dissidents, political opposition and human rights defenders (Shires, 2021a).

While some analysts see commercial spyware as a separate issue to that of cyberwarfare, I treat them as closely linked for two reasons. First, companies selling spyware to states develop 'high-end' capabilities, including rare and expensive exploits of zero-day vulnerabilities, which can equally be used for disruption or targeted assassination as for surveillance alone. Indeed, many associates of Jamal Khashoggi, murdered by Saudi agents in the Saudi consulate in Istanbul, were targeted by such spyware as part of this operation (Marczak et al., 2018). Second, spyware companies often work in close coordination with other intelligence providers, blending technologies and expertise to the extent that it can be difficult to tell where one ends and the other begins. Insofar as digital intelligence capabilities in general are part of cyberwarfare (Brantly, this volume), then, so is spyware.

Furthermore, scholars have demonstrated that private-sector attribution efforts are skewed towards commercial and government clients, and away from civil society (Maschmeyer et al., 2020). This means that there is an attribution gap, filled by organisations such as Citizen Lab,

in which civil society organisations are a major target of such operations, but are least able to defend themselves and least likely to receive external assistance (Anstis et al., 2023).

Citizen Lab investigations use technical investigation, as well as leaks and informants, to reveal the workings of spyware technologies, the location of their suspected state clients, and their connection to human rights violations. In 2014, Citizen Lab developed an innovative method to track software produced by the Italian company Hacking Team (Marczak et al., 2014). They first 'fingerprinted' the surrounding infrastructure, or support servers, for Hacking Team's software, and then sent repeated connection requests to these servers to infer the 'chain' of proxy servers behind the software and their likely geographical country location. In 2015, Citizen Lab published a similar report tracking targeted surveillance software by another company, FinFisher, using equally creative technological tracking (Marczak et al., 2015).

Most notably, Citizen Lab published a mapping report for the Israeli company NSO Group's Pegasus software in 2018, with an even more complex method than the first two (Marczak et al., 2018). They first identified several support servers, then inspected the connection records of these servers to identify targets of the NSO Group operators. This report laid the groundwork for the later Pegasus Project, in which civil society and media organisations revealed Pegasus scandals worldwide, including in many European countries and targeting US government officials in foreign embassies. This project led to an EU Parliamentary inquiry, US sanctions against NSO Group, and lawsuits by individuals targeted and companies whose technologies had been exploited – most notably the Facebook-owned company WhatsApp (Richard and Rigaud, 2023).

Citizen Lab attribution has not been without controversy. NSO Group and other companies threatened legal action multiple times, accusing Citizen Lab not of the defensive act of attribution, but of a more offensive action to hack into the command-and-control

infrastructure behind their spyware. The fingerprinting technique developed by Citizen Lab does go beyond 'home' networks but makes use only of openly available search tools and software. Citizen Lab also undertook extensive internal peer review and technical validation of their fingerprinting technique to counter such misreadings. As well as legal threats, Citizen Lab have also been subject to undercover private investigation and hacking attempts. Crucially, the legal protections afforded by Canadian law and the financial support of the University of Toronto have been essential in maintaining Citizen Lab's work, demonstrating the necessity of academic freedom for civil society's role in cyberwarfare.

Spyware proliferation is now a major concern of many states, with new companies revealed regularly and new markets and centres of development in India, China and Cyprus, to name a few (Feldstein, 2021). Some states have called for international rules and norms on spyware proliferation, signing joint declarations and requiring domestic purchasers to fulfil strict human rights conditions, as well as limiting exports through multilateral agreements such as the Wassenaar Arrangement (DeSombre et al., 2021). While civil society actors such as Citizen Lab were the first to focus on this issue, it now attracts attention from private-sector associations (including the Cyber Tech Accord mentioned earlier), as well as states and multilateral bodies (Naumann, 2023).

Why has the salience of spyware grown in this way? In short, Citizen Lab used their strong attribution evidence to portray human rights violations associated with targeted surveillance as a crucial cybersecurity issue, to counter opponents seeking to prevent the international regulation of surveillance technology exports. Elsewhere, I have called this practice a 'moral manoeuvre,' as it depends not only on rethinking the concept of security but also on mirroring the micro practices, characteristics and genres of cybersecurity (Shires, 2021a).

While Citizen Lab is the most prominent exponent of this practice, they are far from alone. Individuals with experience in analysing state repression during the Arab Spring, in

organisations such as Bahrain Watch, played a key role in subsequent investigations led by Citizen Lab (Marczak, n.d.). Similarly, Amnesty International's renowned digital investigations unit — Amnesty Security Lab – was set up by a researcher with close connections to Citizen Lab (Guarnieri, n.d.). Even beyond the issue of spyware, a wide range of civil society organisations now attribute state and non-state cyber and information operations – including disinformation campaigns and social media influence operations – following the pattern originally established by Citizen Lab.

Importantly, as with the hack-and-leak operations above, not all civil society attributions are what they seem at first glance. An anonymous group named 'Intrusion Truth' has made a name for themselves by attributing Chinese cyber espionage campaigns, claiming to be a group of morally motivated and technically skilled independent analysts (Zetter, 2022). While this is potentially the case, an equally plausible scenario – although with no evidence to confirm it - is that Intrusion Truth acts as a front for Western attributions, whether in the public or private sectors or both (Benincasa, 2023). Other notable examples in this vein come from Iran, with organizations such as Green Leakers and Lab Dookhtegan not only leaking credible information about Iranian cyberwarfare capabilities but claiming to do so as a civil society actor (Greenberg, 2019). In other words, proxy actors are as relevant to cyberwarfare attribution as they are to its conduct.

<b>Civil society and popular mobilisation for cyber conflict

Most examples of supposed popular mobilisation in cyberwarfare are just as accurately understood as proxy actions, along a spectrum of loose encouragement to tight control (Maurer, 2018; Schmoldt, this volume). Early examples of hacktivist DDOS campaigns against Estonia in 2007, or against the US financial sector in 2012-13, fit into this vein. However, Russia's full-scale invasion of Ukraine in 2022 has triggered popular mobilisation for cyber conflict from the Ukrainian side in ways that go beyond concepts of proxy warfare.

The ‘patriotic’ activities of some Russian cybercriminal groups, on the other hand, fall less clearly into this frame, given their close connection to Russian intelligence agencies and my exclusion of criminal groups from the definition of civil society in this chapter more generally (Faife, 2022). Other Russian groups, like the hacking collective KillNet, appear to have only aspirational connections to the Russian government, and are more similar to their Ukrainian equivalents (Antoniuk, 2023).

Although key cyberwarfare contributions have been made by several groups, notably the Belarusian Cyber Partisans, the paradigm example of popular mobilisation for cyberwarfare is Ukraine’s ‘IT Army’ - classified as a threat actor by the Council on Foreign Relations’ popular Cyber Operations Tracker (Council on Foreign Relations, n.d.). Following well-publicised calls to action during the initial invasion, volunteers joined a Telegram channel that grew to over 200,000 members by early 2023 (Tidy, 2023). While the Telegram channel was initially created by a government department, the IT Army is reportedly run by activists who coordinate with Ukraine’s military leaders, rather than taking direct orders (Burgess, 2022). According to interviews, many targets are either suggested by volunteers or come from tip-offs, indicating that this is organic popular mobilisation by civilians on a massive scale, fitting the definition of a civil society movement as much as a military proxy.

Such examples have led to fears of their replication elsewhere in the world, and of the many unintended consequences of popular mobilisation for cyberwarfare. Most notably, the International Committee of the Red Cross (ICRC) has developed the idea of what they term the ‘civilianization of armed conflict’, in cyber as well as other domains (Mačák, 2023). Civilianization means that civilians are increasingly involved in conflicts in new and unpredictable ways, from private-sector cyber defence companies to volunteers for groups such as the IT Army (Soesanto, 2022). Some civil society organisations involved in conflict engage in its broader information dimensions, such as the ‘North Atlantic Fellas

Organisation', an ad-hoc group of volunteers that trolled Russian political figures with cartoon dog avatars on social media, while also taking the more traditional civil society role of raising donations to design the avatars for the Ukrainian military (McInnis et al., 2022).

Many civilian participants in cyberwarfare may be unaware of the risks to which they become exposed, including designation as lawful combatants subject to kinetic military operations as well as retaliation in cyberspace (Biggerstaff, 2023). The legality of these 'cyber militias', like the IT Army, is complex, with advantages on both sides; for either remaining informal and flexible and, conversely, gaining recognition under a state's legal framework (Svantesson, 2023). Interestingly, although some analysts reject legal concepts like the *levee en masse* permitting mass civilian participation as 'a stretch too far' (Väljataga, 2022), such efforts in themselves underline the role of civil society in cyber conflict, as such concepts were developed precisely to legalise armed civil resistance to occupation.

More generally, the civilianization of armed conflict, especially in the cyber domain, increases the risks of horizontal escalation, where conflict spills beyond its original geographic borders (see Libicki and Tkacheva, 2020). While the hacker leadership of Ukraine's IT Army is physically based in Ukraine, this is not the case for all its members, nor for all members of the Cyber Partisans. If such groups launched a significant cyber operation against Russia, this could lead to physical targeting of the country in which they reside. This has significant implications for escalation overall, as NATO has declared that cyber operations could, in certain circumstances, trigger Article 5 of its constitution guaranteeing collective defence of all members (Weidemar, 2023). Popular mobilisation could also lead to vertical escalation, as such groups could – independently of their aligned governments or militaries – take action that leads to more violent and destructive responses by the other side. Finally, it could act as what Owen Jones calls a 'pretext': an excuse or justification for a preplanned diplomatic or military offensive (Jones, 2022).

Overall, popular mobilisation is perhaps the most volatile and fast-moving form of civil society participation in cyberwarfare. In conflicts featuring highly skilled civilian populations, popular mobilisation is highly likely to include cyber operations. Such operations will affect the transnational interdependencies of cyberspace in complex ways, meaning that cyberwarfare develops well beyond its current state-led character.

<b>Conclusion

This chapter has explored several dimensions of civil society's role in and influences on cyberwarfare. Some are relatively indirect, via multilateral or multistakeholder processes seeking to impose rules and norms constraining the conduct of cyberwarfare, or by shaping the overall framing and understanding of cyberwarfare in popular and policy imaginations. Others are more direct, with tactics originating in civil society then used and enhanced by states, and specific kinds of cyberwarfare participation through attribution and popular mobilisation.

To return to the original puzzle posed by this chapter, these influences are not apparent if cyberwarfare is considered to be purely the purview of states, especially military and intelligence agencies; and, conversely, if civil society is understood narrowly as advocacy organisations generally opposed to the expansion of such agencies' powers and remits. Once we broaden our understanding of civil society and look more deeply into the conduct and surrounding environment of cyberwarfare, civil society is a crucial player as both constrainer and enabler.

Even so, this answer to the puzzle remains focused on a single direction of travel for the relationship between civil society and cyberwarfare, treating the former as a participant in and shaper of the latter. The relationship also runs in the other direction. As we see in the discussion of cyber militias, hacktivist groups and other digital conflict parties in the

preceding section, cyberwarfare is generative: it stimulates new forms of civil association, tied closely to specific national contexts but fundamentally transnational in nature. We can apply this generative logic beyond the immediate case of armed conflict. Civil society organizations like Citizen Lab – including their novel combination of technical and political analysis and advocacy - emerge from the unprecedented ways in which states conduct espionage in the digital era and provide a model for democratic participation and influence that can be transplanted to other arenas.

This interrelationship between cyber conflict and civil society raises a further question: how will technological changes in cyber conflict itself – such as the integration of artificial intelligence (AI) into both offence and defence – affect the role and forms of civil society that engage in such conflicts? Here we can return to hack-and-leak operations, and the central role of the media ecosystem in cyberwarfare, for a tentative answer. The impersonation, unauthorized access and strategic leaking described in this chapter is, despite its reliance on cyber intrusions, a relatively manual and small-scale mode of operation. In a media environment characterised not just by mistrust in established discourses, but awash with synthetic media of almost indistinguishable realism, hacking and leaking could become almost unnecessary. Why risk exposure to uncover scandals when inventing them is equally effective? The role of civil society in such a media ecosystem is only beginning to emerge – moving from fact-checkers and content moderators to the independent scrutiny of data collection, algorithmic biases, and new economic models. As cyber conflict embraces AI, these new civil society activities and responsibilities will influence its direction and outcomes. Moreover, as cyber conflict changes with technological advances, so too will civil society – but in ways difficult to anticipate.

Finally, I conclude with a brief personal reflection on civil society and its relevance to cyberwarfare. I do not have experience of the kinds of influence discussed above, from

hack-and-leak operations to attribution or popular mobilisation. However, I have worked with, for, and founded civil society organisations conducting research, advocacy and mediation on cyber conflict. In my experience, cyberwarfare represents a microcosm of the broader dilemma of state relationships faced by civil society organisations across different national contexts. Should they develop close relationships with state counterparts, sharing knowledge, experience and personnel? Or should they cultivate a deliberate separation, mindful of risks of both actual and apparent compromise through association? Each civil society organisation charts a unique path through this dilemma, but those with the most influence seem to avoid both sides, becoming neither proxies nor pure critics. In this, civil society offers a unique space to reflect on cyberwarfare, one which it is vital to preserve.

<b>References

Anstis, Siena, Sophie Barnett, Sharly Chan, Niamh Leonard and Ronald J. Deibert (2023) The negative externalities of cyberspace insecurity and instability for civil society. In James Shires, Max Smeets and Robert Chesney, eds. *Cyberspace and Instability*. Edinburgh: Edinburgh University Press, 240-277.

Antoniuk, Daryna (2023) Killnet as a private military hacking company? For now, it's probably just a dream. *The Record*. 7 July. https://therecord.media/killnet-cybercrime-group-russia-kremlin-hacking-company.

Bauman, Zygmunt, Didier Bigo, Paulo Esteves, Elspeth Guild, Vivienne Jabri, David Lyon and R. B. J. Walker (2014) After Snowden: Rethinking the impact of surveillance. *International Political Sociology* 8(2): 121–144.

Benincasa, Eugenio (2023) Making Cyber Attribution More Transparent. *ETH Zurich Centre for Security Studies Policy Perspectives* 11/5,

https://ethz.ch/content/dam/ethz/special-interest/gess/cis/center-for-securities-studies/pdfs/PP11-5_2023-EN.pdf.

Bernarding, Nina and Viviene Kobel (2023) Feminist Perspectives on the Militarization of Cyberspace. *CFFP (Centre for Feminist Foreign Policy) Policy Brief*. https://centreforfeministforeignpolicy.org/2023/06/21/feminist-perspectives-on-the-militarisation-of-cyberspace/.

Biggerstaff, William Casey (2023) The status of Ukraine's 'IT Army' under the law of armed conflict. *Articles of War*. 10 May. https://lieber.westpoint.edu/status-ukraines-it-army-law-armed-conflict/.

Bishara, Dina (2018) *Contesting Authoritarianism: Labor Challenges to the State in Egypt*. Cambridge: Cambridge University Press.

Brown, Deborah and Allison Pytlak (2020) *Why Gender Matters in International Cyber Security*. Women's International League for Peace and Freedom (WILPF) and the Association for Progressive Communications (APC). https://www.apc.org/sites/default/files/Gender_Matters_Report_Web_A4.pdf.

Burchell, Jon and Joanne Cook (2013) CSR, Co-optation and resistance: the emergence of new agonistic relations between business and civil society. *Journal of Business Ethics*, *115*(4), 741–754.

Burgess, Matt (2022a) Ukraine's volunteer 'IT Army' is hacking in uncharted territory. *Wired.* 27 February. https://www.wired.co.uk/article/ukraine-it-army-russia-war-cyberattacks-ddos.

Burgess, Matt (2022b) Leaked ransomware docs show Conti helping Putin from the shadows. *Wired.* 18 March. https://www.wired.co.uk/article/conti-ransomware-russia.

Campbell, Natalie and Carl Gahnberg (2022) *Impact of Ukraine's requests to block Russia's access to the Internet*. https://www.internetsociety.org/resources/2022/impact-of-ukraines-requests-to-block-russias-access-to-the-internet/.

Chesney, Robert and Max Smeets, eds. 2023) *Deter, Disrupt or Deceive: Assessing Cyber Conflict as an Intelligence Contest.* Washington, DC: Georgetown University Press.

Coleman, Gabriella (2014) *Hacker, Hoaxer, Whistleblower, Spy: The Many Faces of Anonymous*. London: Verso.

Council on Foreign Relations (n.d.) Ukrainian IT Army. https://www.cfr.org/cyber-operations/ukrainian-it-army.

Deibert, Ronald J. (2018) Toward a human-centric approach to cybersecurity. *Ethics & International Affairs* 32(4): 411–24.

Deibert, Ronald J. (2020) *Reset: Reclaiming the Internet for Civil Society*. Toronto, ON: House of Anansi Press.

DeSombre, Winnona, James Shires, J.D. Work, Robert Morgus, Patrick Howell O'Neill, Luca Allodi and Trey Herr (2021) *Countering Cyber Proliferation: Zeroing in on Access-as-a-Service.* Washington, DC: Atlantic Council Cyber Statecraft Initiative. https://www.atlanticcouncil.org/in-depth-research-reports/report/countering-cyber-proliferation-zeroing-in-on-access-as-a-service/.

Devanny, Joe, Ciaran Martin and Tim Stevens (2021) On the strategic consequences of digital espionage, *Journal of Cyber Policy* 6(3): 429-450.

Diamond, Larry (1994) Rethinking civil society: Toward democratic consolidation. *Journal of Democracy* 5(3): 4-17.

Dunn Cavelty, Myriam (2019) The materiality of cyberthreats: Securitization logics in popular visual culture. *Critical Studies on Security* 7(2): 138–51.

Egloff, Florian J. and Myriam Dunn Cavelty (2021) Attribution and knowledge creation assemblages in cybersecurity politics. *Journal of Cybersecurity* 7(1): tyab002.

Eringfeld, Simone (2021) Higher education and its post-coronial future: Utopian hopes and dystopian fears at Cambridge University during Covid-19. *Studies in Higher Education* 46(1): 146-157.

Faife, Corin (2022) A ransomware group paid the price for backing Russia. *The Verge.* 22 February. https://www.theverge.com/2022/2/28/22955246/conti-ransomware-russia-ukraine-chat-logs-leaked.

Feldstein, Steven (2021) *The Rise of Digital Repression: How Technology Is Reshaping Power, Politics, and Resistance*. New York: Oxford University Press.

FireEye Intelligence (2018) TRITON Attribution: Russian government-owned lab most likely built custom intrusion tools for TRITON attackers. 23 October. https://www.mandiant.com/resources/blog/triton-attribution-russian-government-owned-lab-most-likely-built-tools.

Gellman, Barton (2021) *Dark Mirror: Edward Snowden and the American Surveillance State.* New York: Penguin Random House.

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.

Gorwa, Robert (2019) The platform governance triangle: Conceptualising the informal regulation of online content. *Internet Policy Review* 8(2). https://doi.org/10.14763/2019.2.1407.

Greenberg, Andy (2019) A mystery agent is doxing Iran's hackers and dumping their code. *Wired.* 18 April. https://www.wired.com/story/iran-hackers-oilrig-read-my-lips/.

Guarnieri, Claudio (n.d.) Nex. https://github.com/sponsors/botherder.

Habermas, Jürgen (2006) Political communication in media society: Does democracy still enjoy an epistemic dimension? The impact of normative theory on empirical research. *Communication Theory* 16 (4): 411–426.

Hakmeh, Joyce and Patryk Pawlak (2021) Cybercrime negotiations: Affairs beyond states. *Directions*. 29 January. https://directionsblog.eu/cybercrime-negotiations-affairs-beyond-states/.

Harknett, Richard J. and Max Smeets (2022) Cyber campaigns and strategic outcomes, *Journal of Strategic Studies* 45(4): 534-567.

Healey, Jason, ed. (2013) *A Fierce Domain: Conflict in Cyberspace, 1986 to 2012*. Vienna, VA: Cyber Conflict Studies Association.

Hurel, Louise Marie and Luisa Cruz Lobato (2018) Unpacking cyber norms: Private companies as norm entrepreneurs. *Journal of Cyber Policy* 3(1): 1–16.

Johnson, Derek B. (2022) Major tech groups, nonprofits iced out of UN working group on cybersecurity norms. *SC Magazine*. 22 July. https://www.scmagazine.com/analysis/major-tech-groups-nonprofits-iced-out-of-un-working-group-on-cybersecurity-norms.

Jones, Marc Owen (2022) *Digital Authoritarianism in the Middle East: Deception, Disinformation and Social Media*. London: Hurst.

Jongen, Hortense and Jan Aart Scholte (2022) Inequality and legitimacy in global governance: an empirical study. *European Journal of International Relations* 28(3): 667–95.

Judson, Ellen, Asli Atay, Alex Krasodomski-Jones, Rose Lasko-Skinner and Josh Smith (2020) *Engendering Hate: The Contours of State-Aligned Gendered Disinformation Online*. London: Demos. https://demos.co.uk/research/engendering-hate-the-contours-of-state-aligned-gendered-disinformation-online/.

Keck, Margaret E. and Kathryn Sikkink (1998) *Activists beyond Borders: Advocacy Networks in International Politics*. Ithaca, NY: Cornell University Press.

Kelty, Christopher M. and Gabriella Coleman (2017) Preface: Hacks, leaks, and breaches. *Limn* 8. https://limn.it/articles/preface-hacks-leaks-and-breaches/.

Knight, Sam (2019) How Football Leaks is exposing corruption in European soccer. *The New Yorker*. 27 May. https://perma.cc/CS75-BA45.

Kumar, Sheetal (2021) The missing piece in human-centric approaches to cybernorms implementation: the role of civil society. *Journal of Cyber Policy* 6(3): 375–93.

Lavie, Limor and Bosmat Yefet (2022) The relationship between the state and the new media in Egypt: a dynamic of openness, adaptation, and narrowing. *Contemporary Review of the Middle East* 9(2): 138-157.

Libicki, Martin C. and Olesya Tkacheva (2020) Cyberspace escalation: Ladders or lattices? In Amy Ertan, Kathryn Floyd, Piret Pernik and Tim Stevens, eds. *Cyber Threats and*

NATO 2030: Horizon Scanning and Analysis. Tallinn: NATO CCD COE Publications, 60-72.

Liebetrau, Tobias and Linda Monsees (2023) Assembling publics: Microsoft, cybersecurity, and public‐private relations." *Politics and Governance* 11 (3): 157–67.

Lomashvili, Masho (2022) In Israel, ransomware attacks against private companies pose a new kind of national security threat. *Coda Story*. 20 January. https://www.codastory.com/disinformation/iran-israel-ransomware/.

Lyon, David (2015) *Surveillance after Snowden*. Cambridge: Polity.

Mačák, Kubo (2023) Will the centre hold? Countering the erosion of the principle of distinction on the digital battlefield. *International Review of the Red Cross* 105(923): 965-991.

Mainwaring, Sarah and Richard J. Aldrich (2021) The secret empire of signals intelligence: GCHQ and the persistence of the colonial presence. *The International History Review* 43(1): 54-71.

Marczak, Bill (n.d.) https://billmarczak.org/.

Marczak, Bill, Claudio Guarnieri, Morgan Marquis-Boire and John Scott-Railton (2014) Mapping Hacking Team's 'untraceable' spyware. *The Citizen Lab*. 17 February. https://citizenlab.ca/2014/02/mapping-hacking-teams-untraceable-spyware/.

Marczak, Bill, John Scott-Railton, Sarah McKune, Bahr Abdul Razzak and Ronald J. Deibert (2018) Hide and Seek: Tracking NSO Group's Pegasus Spyware to Operations in 45 Countries. Toronto: The Citizen Lab. https://munkschool.utoronto.ca/research/hide-and-seek-tracking-nso-groups-pegasus-spyware-operations-45-countries.

Marczak, Bill, John Scott-Railton, Adam Senft, Ronald J. Deibert, and Bahr Abdul Razzak (2018) The Kingdom Came to Canada: How Saudi-Linked Digital Espionage Reached Canadian Soil. Toronto: The Citizen Lab. https://citizenlab.ca/2018/10/the-kingdom-came-to-canada-how-saudi-linked-digital-espionage-reached-canadian-soil/.

Marczak, Bill, John Scott-Railton, Adam Senft, Irene Poetranto and Sarah McKune (2015) *Pay No Attention to the Server behind the Proxy: Mapping FinFisher's Continuing Proliferation*. Toronto: The Citizen Lab. https://citizenlab.ca/2015/10/mapping-finfishers-continuing-proliferation/.

Maschmeyer, Lennart, Ronald J. Deibert and Jon R. Lindsay (2021) A tale of two cybers: How threat reporting by cybersecurity firms systematically underrepresents threats to civil society. *Journal of Information Technology & Politics* 18(1): 1–20.

Maurer, Tim (2018) *Cyber Mercenaries: The State, Hackers, and Power*. Cambridge: Cambridge University Press.

McInnis, Kathleen, Seth G. Jones and Emily Harding (2022) *NAFO and Winning the Information War: Lessons Learned from Ukraine*. Washington, DC: Centre for Strategic & International Studies. https://www.csis.org/analysis/nafo-and-winning-information-war-lessons-learned-ukraine.

Menn, Joseph (2020) *Cult of the Dead Cow: How the Original Hacking Supergroup Might Just Save the World*. New York: PublicAffairs.

Millar, Katharine M., James Shires and Tatiana Tropina (2021) *Gender Approaches to Cybersecurity: Design, Defence and Response*. Geneva: UN Institute for Disarmament Research (UNIDIR). https://unidir.org/publication/gender-approaches-to-cybersecurity/.

Naumann, Saher (2023) Countering Irresponsible Cyber Proliferation. *BAE Systems Digital Intelligence.* 25 October. https://www.baesystems.com/en/digital/blog/countering-irresponsible-cyber-proliferation.

Oever, Niels ten (2019) Productive contestation, civil society, and global governance: Human rights as a boundary object in ICANN. *Policy & Internet* 11(1): 37–60.

Oliveira, Gabriela de and Julia Slupska (2023) *The Digital Misogynoir Report: Ending the Dehumanising of Black Women on Social Media*. London: Glitch. https://glitchcharity.co.uk/wp-content/uploads/2023/07/Glitch-Misogynoir-Report_Final_18Jul_v5_Single-Pages.pdf.

Poetranto, Irene (2019) Narrative and politics of hacking in WarGames, Sneakers, and Blackhat." *Public Voices* 16(1): 21–36.

Porta, Donatella Della and Sidney Tarrow, eds. (2004) *Transnational Protest and Global Activism*. Lanham, MD: Rowman and Littlefield.

Raiu, Costin, Daniel Moore, Juan Guerrero-Saade and Thomas Rid (2017) *Penquin's Moonlit Maze: The Dawn of Nation-State Digital Espionage*. Kaspersky, GREAT and King's College London. https://media.kasperskycontenthub.com/wp-content/uploads/sites/43/2018/03/07180251/Penquins_Moonlit_Maze_PDF_eng.pdf.

Raymond, Mark and Laura DeNardis (2015) Multistakeholderism: Anatomy of an inchoate global institution. *International Theory* 7(3): 572–616.

Richard, Laurent and Sandrine Rigaud (2023) *Pegasus: The Story of the World's Most Dangerous Spyware.* London: Macmillan.

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

Ruhl, Christian, Duncan B. Hollis, Wyatt Hoffman and Tim Maurer (2020) *Cyberspace and Geopolitics: Assessing Global Cybersecurity Norm Processes at a Crossroads*. Washington, D.C: Carnegie Endowment for International Peace. https://carnegieendowment.org/2020/02/26/cyberspace-and-geopolitics-assessing-global-cybersecurity-norm-processes-at-crossroads-pub-81110.

Schneier, Bruce (2015) The rise of political doxing. *Schneier on Security*. 2 November. https://www.schneier.com/blog/archives/2015/11/the_rise_of_pol.html.

Shires, James (2019) Hack-and-leak operations: Intrusion and influence in the Gulf. *Journal of Cyber Policy* 4(2): 235–56.

Shires, James (2020a) Cyber-noir: Cybersecurity and popular culture. *Contemporary Security Policy* 41(1): 82–107.

Shires, James (2020b) The simulation of scandal: Hack-and-leak operations, the Gulf States, and US politics. *Texas National Security Review* 3(4): 10-29.

Shires, James (2021a) *The Politics of Cybersecurity in the Middle East*. London: Hurst.

Shires, James (2021b) Windmills of the mind: Higher-order forms of disinformation in international politics. In *2021 13th International Conference on Cyber Conflict (CyCon)*. https://doi.org/10.23919/CyCon51939.2021.9468292.

Shires, James and Michael McGetrick (2021) *Rational Not Reactive: Re-Evaluating Iranian Cyber Strategy.* Cambridge, MA: Harvard Kennedy School. https://www.belfercenter.org/publication/rational-not-reactive.

Soesanto, Stefan (2022) *The IT Army of Ukraine: Structure, Tasking, and Ecosystem.* ETH Zurich Centre for Security Studies Cyberdefence Report. https://css.ethz.ch/content/dam/ethz/special-interest/gess/cis/center-for-securities-studies/pdfs/Cyber-Reports-2022-06-IT-Army-of-Ukraine.pdf.

Stoll, Cliff (2005 [1989]) *The Cuckoo's Egg: Tracking a Spy Through the Maze of Computer Espionage*. New York: Gallery Books.

Svantesson, Dan Jerker B. (2023) Regulating a 'cyber militia': Some lessons from Ukraine, and thoughts about the future. *Scandinavian Journal of Military Studies*, 6(1): 86–101.

Tidy, Joe (2023) Meet the hacker armies on Ukraine's cyber front line. *BBC News*. 14 April. https://www.bbc.com/news/technology-65250356.

Väljataga, Ann (2022) Cyber vigilantism in support of Ukraine: a legal analysis. Tallinn: NATO Cooperative Cyber Defence Centre of Excellence (CCDCOE). https://ccdcoe.org/uploads/2022/04/Cyber-vigilantism-in-support-of-Ukraine-a-legal-analysis.pdf.

Weidemar, Sarah (2023) NATO and Article 5 in Cyberspace. *ETH Zurich Centre for Security Studies Analyses in Security Policy* 323. https://css.ethz.ch/content/dam/ethz/special-interest/gess/cis/center-for-securities-studies/pdfs/CSSAnalyse324-EN.pdf.

Zetter, Kim (2022) Intrusion Truth: Five years of naming and shaming China's spies. *Zero Day.* 29 March. https://www.zetter-zeroday.com/p/interview-with-intrusion-truthzetter.