On the Peace and Security Implications of Cybercrime: A Call for an Integrated Perspective

Hansel, Mischa; Silomon, Jantje

Veröffentlichungsversion / Published Version
Forschungsbericht / research report

Empfohlene Zitierung / Suggested Citation:
Hansel, M., & Silomon, J. (2023). *On the Peace and Security Implications of Cybercrime: A Call for an Integrated Perspective.* (IFSH Research Report, 12). Hamburg: Institut für Friedensforschung und Sicherheitspolitik an der Universität Hamburg (IFSH). https://doi.org/10.25592/ifsh-research-report-012

IFSH
Institute for Peace Research
and Security Policy
at the University of Hamburg

RESEARCH REPORT
#012

On the Peace and Security Implications of Cybercrime
A Call for an Integrated Perspective

MISCHA HANSEL / JANTJE SILOMON | 04/2023

Table of Contents

Abstract

Criminal cyberattacks have skyrocketed in the past decade, with ransomware attacks during the pandemic being a prime example. While private corporations remain the main targets and headlines are often dominated by the financial cost, public institutions and services are increasingly affected. Governments across the globe are working on combatting cybercrime. However, they often do not see eye-to-eye, with geopolitical tensions complicating the search for effective multilateral remedies further. In this research report, we focus on the threat that cybercrime poses to peace and security, which is rarely addressed. We examine the potential of cybercrime to exacerbate state-internal conflicts, for example by fuelling war economies or by weakening social coherence and stability. Various actors sharing similar, possibly even identical, approaches to compromising adversarial computer systems is another threat that we assess, as it has the potential to cause unintended escalation. Similarly, cyber vigilantism and hack-backs, whether conducted by private actors or corporate entities, can also endanger state agency and the rule of law. While an international treaty, as for example currently being discussed at the UN, could be a valuable step toward curbing cybercriminal behaviour, we also reflect on possible negative side effects – from increased domestic surveillance to repression of opposition. Lastly, we argue for an integrated perspective, combining various knowledge bases and research methodologies to counter direct and indirect limitations of research, particularly pertaining to data availability but also analytical concepts.

Keywords: Cybercrime, Ransomware, Cybersecurity, Conflict Escalation, War against Ukraine, Law Enforcement, Domestic Repression, UN Cybercrime Convention

Funding

This report was produced as part of the research focus “International Cybersecurity” funded by the German Federal Foreign Office.

1 Introduction

Spectacular ransomware attacks during the COVID-19 pandemic accentuated the growing problem of cybercrime, affecting energy provision, food supplies, healthcare services and public administrations. While the private sector remains the predominant target, with annual economic losses estimated at 200 billion Euros in Germany alone (Bitcom 2022), public institutions and services are increasingly becoming victims, sometimes unintentionally so. A large proportion of these attacks affect essential and time-sensitive services, often resulting in vulnerable parts of society suffering the most, such as when an attack against the German district of Anhalt-Bitterfeld in 2021 made social and housing benefit payments impossible (Heidtmann 2021). In 2022, the criminal ransomware gang Conti attacked 27 state-led institutions in Costa Rica and even threatened to overthrow the government, forcing the latter to declare a state of national emergency (Euronews 2022). Other attacks, such as on hospitals in Ireland, greatly impacted public health services at a time when medical capacities were already strained (Perlroth and Satariano 2021).

Economic cost estimates of cybercrime often overlook these social consequences. The potential impact on peace and security is even less well understood. Recent cases, however, show that cybercrime operations create collateral damage across borders, leaving ample room for misperception and unintended escalation. Against this background, cybercrime has to be understood as a truly global phenomenon with potential repercussions on conflict prevention and crisis management. While state actors should all be inclined to address these challenges, at least in theory, finding practical solutions remains anything but an easy task. Informal relationships between various state security agencies, primarily within authoritarian governments, and actors within the criminal cyber underground offer tactical and strategic benefits to both sides. As a result, some governments show a tendency towards obstructing real progress on international law enforcement cooperation or strengthening principles of state due diligence in cyberspace.

Institutional path-dependencies can also complicate the search for effective multilateral remedies. Since 2004, various Groups of Governmental Experts (GGE) have come together to discuss cyber threats to inter-state peace within the United Nations General Assembly's (UNGA's) First Committee. These talks resulted in the establishment of 11 voluntary norms of responsible state behav-

iour in cyberspace as well as other practical suggestions to avoid inter-state escalation. While discussions on the peace and security aspects of state behaviour continued among official state representatives within the Open Ended Working Group (OEWG) from 2019 onwards, Russia initiated a separate negotiation process on a legally binding UN cybercrime convention within UNGA's Third Committee. There are thus two separate negotiation processes dealing with the avoidance of interstate escalation and the fight against cybercrime, respectively, despite substantial overlap between these areas. Furthermore, Western states have been reluctant to create institutional linkages between the two negotiation agendas, fearing that provisions within a future legally binding UN cybercrime convention could be deliberately designed to undermine the voluntary cyber norm acquis developed within UNGA's First Committee.

Ongoing negotiations within the UN are therefore structured around an artificial divide between state responsibilities on the one hand and threats posed by non-state actors on the other. This is despite the fact that in many cases state agencies themselves rely on the services of cybercriminals or even orchestrate their cyber campaigns (Maurer 2018). Against this background, our study considers various alternative mechanisms that could complement or substitute multilateral efforts at UN level. At the same time, we also need to consider a potential dark side of international cooperation against cybercrime, whether within or beyond the UN. Many civil society organisations worry about the outcome of ongoing negotiations on a UN cybercrime convention (Electronic Frontier Foundation et al. 2023; Pavlova and Lindsey 2023). A key concern is that under certain conditions, such as vaguely defined crimes and lack of procedural safeguards, international commitments could embody peace and security risks themselves, for example, by serving as a pretext for state-led violence in authoritarian regimes. Studying peace and security risks of cybercrime therefore requires considering both direct and indirect effects, the latter including the use of cybercrime as a cover for domestic repression.

After a brief discussion of concepts and definitions, our research report presents evidence of various peace and security risks that result from global cybercrime trends. Following each trend analysis, we also assess the problem-solving effectiveness of existing cooperation regimes and alternative frameworks against the background of our observed implications and impacts of cybercrime. Beyond anchoring the study of cybercrime more firmly in international security studies scholarship, the goal of our report is to argue for an integrated perspective on

the nexus of cybercrime, peace, and security, encompassing disciplines as diverse as computer science, political science, and criminology. We will thus point out the practical challenges of such an integrated perspective towards the end of our analysis, from rediscovering bodies of knowledge that have long been neglected to the need to bridge diverging standards and agree on a common set of research goals that merit more intensive study. The conclusion of our study summarises our main results and provides a final assessment of the promises and potential pitfalls of the ongoing negotiations on a cybercrime convention within the UN Ad Hoc Committee[1].

2 Cybercrime – A Growing Threat to Peace and Security

Cybercriminals, intelligence agencies, so-called hacktivists and military cyber units all seek to gain unauthorised access to third party computer systems and networks. The threats posed by such activities and the security measures against them define a core element of the broader field of cybersecurity. Differentiating actors can be challenging as they utilise similar, or even the same, tactics, techniques, and procedures (TTPs)[2] when attacking a system, despite greatly varying motivations: cybercriminals, are mostly driven by financial aspects, unlike for example intelligence agencies engaged in espionage activities. At times, tools and services are also used by various actors, particularly if they rely (at least in part) on malware-as-a-service (Sadowski 2023). To complicate matters further, cybersecurity professionals and researchers often rely on some of the same tools to analyse nefarious actors or secure systems. Given this shared use of resources and the difficulty in determining an actor's intentions, it is not surprising that these levels of uncertainty greatly complicate policy responses, particularly given the growing number and sophistication of cyberattacks. We will discuss this aspect in more detail in our analysis of institutional responses, but here, suffice it to say that the same ambivalence also creates methodological challenges for researchers.

In the light of these uncertainties, it is therefore hardly surprising that the estimates of costs incurred specifically by cybercrime as opposed to other types of cyberattacks differ greatly. Yet, the numbers point to a very clear trend. Thus, the global economic costs caused by cybercrime (broadly defined) surged from an estimated 300 billion US dollars in 2013 to almost 1 trillion US dollars in 2020, representing just over 1% of global GDP, according to a McAfee study (Smith et al. 2020: 3). Another study estimated the global economic costs of cybercrime at 3 trillion US dollars in 2015 already, with a projected rise to 10.5 trillion US dollars by 2025. If accurate, the profitability of cybercrime would then surpass that of the global trade of illegal drugs (Morgan 2020). At the same time, the enforcement gap (the probability of not being convicted) is much higher for cybercrime than for selling drugs (Eoyang et al. 2018). While these figures are worrisome, they still only tell one part of the whole story, i.e. the one centred on

economic damages and lost economic opportunities. The wider social impact, and in particular a focus on the relationship between cybercrime and violence, is missing from these accounts.

Crime arguably has always had peace and security implications and is deeply intertwined with politics (Barnes 2017; Locke 2012), be it through illegitimate diversion of public money (corruption) that otherwise would help to keep social divisions within certain limits, or through criminals subverting state monopolies of violence (as for example drug cartels in Mexico). Assessing the impact of the cyber dimension is challenging not only because there are wide disagreements on the boundaries of the concept (see Brady and Heinl 2020: 17–22) but also because academic studies and empirical data is lacking. A very narrow definition of cybercrime would only include profit-oriented attacks against the confidentiality, integrity, and availability (CIA) of computer systems and digital data ("crimes against computers" or cyber-dependent crimes). A broader definition, in contrast, would also include digital operation modes and distribution channels of traditional criminal enterprises, as for example online drug trading or online fraud ("crimes committed by use of computer" or cyber-enabled crimes) (United Nations Office on Drugs and Crime n.d.). Finally, domestic cybercrime legislation as well as international law enforcement further tackle content-related offenses, for example the posting of child pornography or social media incitement to hatred.

Our research report primarily deals with the first category, cyber-dependent crimes as their characteristics and effects are unique in many ways. For example, they rely on the global malware ecology or share numerous techniques with state-led cyber operations, making the two often hard to distinguish from each other (see below). Such peculiarities deserve particular attention in our view, since they limit the applicability of existing public policy and international security templates. That having been said, we cannot ignore the fact that many policy-makers, law enforcement agencies, and other practitioners have a responsibility to deal with all types of cybercrime at once. Nor can we overlook the politics around the boundaries of the concept as we discuss further below. Finally, there are cases where the evidence of the impact of cyber-enabled crimes is much stronger, such as the online trading of illicit goods. Consequently, we will then also assess the impact on peace and security of those other types of cybercrime.

2.1 EXACERBATING INTERNAL CONFLICTS AND CIVIL WAR DYNAMICS

One way to assess the peace and security implications of cybercrime is to look at its impact on already conflict-prone societies. Conventional wisdom would not expect countries with low income to rank high on the list of victims of cyber-dependent crimes. To some degree this is true. For example, recent data on phishing in a business context shows that African victims account for less than 1% of victims worldwide (Interpol 2021: 18). Yet, this is likely to change with growing internet penetration rates (Swiatkowska 2020: 9). As a consequence, cybercrime is 'catching up' while at the same time having regional characteristics. For example, financial institutions are among the top targeted industry in Africa due to rapid digitalisation in recent years (Interpol 2022: 5, CNBC Africa 2021). Moreover, Africa also suffers from one of the highest growth rates in detected ransomware attacks, as well as increasing DDoS attacks against critical infrastructures (Interpol 2021: 9, 21–23; Delcker 2022).

Cybercrime in developing regions is often facilitated by limited security investments alongside of poorly defended systems. Furthermore, many of these systems utilise illegal software copies which may come riddled with malware or simply compromise the system by not allowing for regular updates and patches (Kshetri 2019: 77–78). There is also clear evidence that the lack of economic opportunities within many developing countries works as a pull-factor in attracting skilled computer specialists. But it also attracts non-specialists to cybercrime (Ilievski and Bernik 2016; Kshetri 2010), a tendency further strengthened by the COVID-19 pandemic (Kaspersky 2023). Some also argue that cybercrime, in turn, aggravates poverty and thus weakens social coherence and stability, either because people with low income cannot afford technical or legal protection (Baer 2017) or because of lost development opportunities at the societal level (Swiatkowska 2020; World Economic Forum 2020: 6). Here again ransomware, for example, is also used to disrupt and demand payments from public schools, medical services and local administrations – basic public goods that people with low income are more dependent on than those with higher income. Moreover, given that in many world regions such public services are already strained and unlikely to meet actual demand, the disruption caused by cybercrime (and the costs needed to prevent it) will potentially aggravate already existing distributional conflicts. There is also an argument that cybercrime spikes around 'natural disasters', pandemics, and periods of civil unrest, exploiting feelings of

anxiety and helplessness (Wong 2020). Here similarly, low income-households within developing countries often face higher risks during such events, causing cybercrime to have a particularly destabilising impact in some world regions.

Nonetheless, the most serious impact of cybercrime on peace and security in developing regions is likely indirect, by fuelling war economies on the one hand and destabilising societies through the spread of disinformation and violent propaganda on the other. A recent Interpol study underlines the first assertion, showing that the internet and social media are increasingly used for illegal wildlife trade as well as the trafficking of drugs and 'blood diamonds' in African countries (Interpol 2021: 33–38, see also Allen 2021). Through this, cyber-enabled criminal operations arguably add to the 'resource course' of many war-torn societies by creating vicious circles of civil violence and resource extraction (Ross 2015). They also contribute to immediate security risks by spreading small and light weapons throughout the continent (Interpol 2021: 35–36). With regard to the second element, there is a growing literature on the role of violence-incitement through social media in conflict-ridden and fragile societies and regions. A case in point is the role of hate speech and disinformation in the campaign against the Rohingya minority in Myanmar (Rio 2020). However, whether or not such messages are criminalised depends on national laws. A related challenge to peace and security stems from covert influence operations, reaching far beyond Western countries. For example, manipulative micro-targeting activities of foreign data companies bear significant responsibility for polarisation and electoral violence in Kenya in 2013 and 2017 (Nyabola 2018: 160–167).

Moving from description to tentative policy responses, addressing the risks of cybercrime within fragile and/or developing regions needs to consider the peculiar vulnerabilities, attack vectors, and criminal incentives in each particular country. International cooperation would be beneficial in many cases, yet a crucial capacity gap needs to be overcome; for example, few African states have developed a cybersecurity strategy (Ifeanyi-Ajufo 2022). Furthermore, many law enforcement agencies, especially in the Global South, are overburdened with processing Mutual Legal Assistance requests (Rodriguez 2017). Developed countries could probably do more to address this issue – for example, by committing to provide more technical and financial assistance while at the same time pledging to align their own staffing with growing numbers of data retention or disclosure requests. Such pledges could take the form of political commitments within a negotiated agreement, with the added value of working

as standard-setting and donor-coordination mechanisms (Peters and Garcia 2020: 55) respectively. Another useful option would be to share the benefits of existing prioritised cross-border investigation mechanisms with a larger number of developing countries. For example, Colombia is already one of several non-EU partner countries within Europol's Joint Cybercrime Action Taskforce (J-CAT). Prioritising some cases on the basis of their particular peace and security risks would be another way to create a more equitable institutionalisation of cross-border investigations. Existing partnerships, for example between the European Union and the Economic Community of West African States (ECOWAS) should be leveraged to create a facilitating policy environment for such cooperation (Ifeanyi-Ajufo 2022). While actual decision-making on prioritisation would always be done on a case-by-case basis, the development of a new classification scheme, focussing specifically on peace and security impacts, could offer helpful guidance. The 'elephant in the room' from an inter-regional cooperation perspective however will be offering market access, development opportunities, and fairer terms of trade, enabling African economies to absorb vast numbers of young and digitally literate people, and thus counteract the recruitment efforts of cybercriminal networks.

While we have primarily focussed on domestic peace so far, the following parts will address international aspects in more detail. Most cybercrime operations operate across borders, not only to gain access to lucrative targets but also to escape law enforcement.

2.2 UNINTENDED ESCALATION AND ACTOR AMBIGUITY

Avoiding unintended escalation and facilitating multilateral crisis management has been one of the key priorities of international cyber-diplomacy in recent years. For example, the risk of false flag operations, where attackers disguise themselves as another group or even state adversaries in order to provoke counterattacks against innocent third parties, is growing, or at least appears to be given a number of recent cases (see for example O'Neill 2021a). Other escalation risks may result from collateral damage. A telling estimate was given by ENISA's executive director in June 2022, saying that a third of observed cyber events in the context of the Russian war in Ukraine were actually "spill-over inci-

dents", affecting sectors and systems other than what seemed to have been the primary targets (Kabelka 2022a). In the absence of effective confidence-building measures and emergency communication channels, such risks might, under unfavourable circumstances, evolve into a serious international crisis.

2.2.1 BLURRED LINES BETWEEN CRIME AND GEO-POLITICS

Looking at the empirical record of actual cyberattacks, one might argue that the overall probability of crisis escalation is rather low, at least with regard to the risk of kinetic responses. Indeed, no state has ever claimed to have suffered from a cyber-operation that crossed the threshold of the use of force in international law, thus legitimising kinetic countermeasures (Delerue 2020). Instead of reacting with countermeasures, states tend to respond with measures of retorsion, if at all. This includes sanctions, indictments, or diplomatic protest. Albania's decision to suspend all diplomatic relations with Iran in response to a series of cyberattacks has possibly been "the strongest public response to a cyberattack we have ever seen" (John Huttquist, Vice President of Mandiant, quoted in Reuters 2022). Yet even if we include such instances of political escalation, quantitative empirical studies, and simulations do not appear to support the notion of substantial offline escalation potential of cyberattacks (see for example Jensen and Valeriano 2019; Valeriano and Maness 2014). That said, neither past patterns nor experimental findings necessarily predict future interactions. Nor do they have to guide policy decisions. The fact that the application of the right to self-defence has been one of the most contentious issues within UN cyber norm building processes is telling in this regard. As is the publication of national viewpoints on the application of international law in cyberspace, making it very clear that at least from the perspective of some states, particularly destructive cyberattacks can be classified as violations against the rule not to use force in international relations (Glick and Simon 2022). Finally, strategic circumstances matter. A case in point is the return of great power military conflict in the wake of the Russian invasion of Ukraine. Statements such as the Russian warning that cyberattacks on militarily used satellites would constitute an act of war might be primarily intended to intimidate Western audiences (Bender 2022). Yet at the same time, they might also indicate a shift in perceptions and shape expectations with regard to the strategic value of critical IT infrastructures. Another case in point is US President Biden's 2021 warning of a "real shooting war with a great

power" as the result of a future cyber breach (The White House 2021). Overall, it would be farfetched to dismiss the possibility of a serious offline escalation due to future cyberattacks, especially during geopolitical crises. This in turn implies the risk of grave peace and security risks due to misattributions and misperceptions.

With cybercrime and ransomware operations in particular entering into the equation, the situation is further aggravated. This is not to say that cybercriminals do not have an incentive to limit the damage done. On the contrary, cybercriminals do not benefit from growing awareness at the political level since countermeasures are likely to increase operational costs. At the same time, though, the division of labour within cybercrime markets (cybercrime-as-a-service) not only increases the volatility and anonymity within cybercrime operations (Collier 2021; ENISA 2022: 17). It could also outbalance the above-mentioned security considerations since brokers of initial access to computer systems, providers of botnets, and sellers of ransomware services compete for clients. The intensity of this competition is mirrored in falling prices for malware, DDoS-attacks, forged documents, and other criminal tools and products.[3] In the long run, the most reckless sellers might outcompete those that are more cautious. Newcomers can skip ahead of established criminal brands by buying instead of building their arsenals for attack (Carmi 2022). Alternatively, they may rebuild on operations shut- down by law enforcement, for example, either due to key members not having been taken into custody or sufficient infrastructure remaining viable for criminal use. There is, however, the possibility that their lack of experience can result in collateral damage amongst other things. For example, there are several cases where attacks on hospitals might have happened by mistake. While ransomware operators responded by issuing decryption keys for free, this did not limit disruptive effects, at least not in the short term (CyberPeace Institute 2021).

This modus operandi creates structurally similar risks to peace and security as pre-delegated military authority or disloyal military commanders (Feaver and Geers 2017). Incompetent or reckless operatives on any level can cause excessive or unintended damage. Even with adequate oversight in place, the characteristics of some types of cyberattacks, such as those inserting malware in supply chains, make it challenging to anticipate and control real-world consequences (Tait 2021). A similar peace and security risk relates to human cognition and how it supports perception biases when assessing cybercrime and cyberattacks in general (Hansel 2018). More specifically, humans are prone to confirmation

biases and a tendency to overestimate the organisational coherence of adversarial campaigns. Because of such tendencies, there is a possibility that a criminal cyber operation or its effects will be misperceived as evidence of top-level authorised political attacks. From a defender's point of view, the dilemma here is to avoid both false positives (miscategorising cybercrime as political attacks) and false negatives (misperceiving political attacks as cybercrime). That such ambivalences create real uncertainties is shown by a 2021 survey of 800 IT security decision makers in the United States, the United Kingdom, Germany, France, Japan, India, and Australia. Although the majority of respondents emphasised the importance of distinguishing between state-based attacks and others, only around one in four claimed to have complete confidence in the ability of their organisation to do so (Trellix 2022: 13–14).

Recent trends have only worsened this dilemma by blurring the lines between cybercrime and politically motivated cyber operations even further. While tacit support or active sponsorship of criminal cyber proxies has long been used as a force multiplier and as a way to achieve 'plausible deniability' by some authoritarian states in particular (Maurer 2018; Lachow and Grossman 2018: 393), ransomware is likely to create much stronger synergies (Jun 2021; Handler 2021). In fact, several past attacks are hard to classify as either cybercrime or politically motivated sabotage. For example, in May 2021, security researchers discovered a disk-wiping malware of Iranian origin disguised as ransomware targeting Israeli systems. The ultimate goal of this cyber operation, they speculated, never was to provide decryption in exchange for money but instead cause long-term disruption (Goodin 2021). In 2022, alleged Chinese state-affiliated hacking groups reportedly used ransomware as a decoy to obscure their tracks and to complicate attribution rather than to blackmail their victims in Japan, Europe and the United States (Toulas 2022).[4] Back in 2017, NotPetya inflicted billions of US dollars in damages worldwide. But according to some security researchers, it likely was not a profit-generating venture given the ransom was comparatively low and some data was irretrievable. Instead, the primary aim of the operation was to quickly damage predominantly Ukrainian targets (BBC 2017; Goodin 2017). In 2021, the Commander of the French Cyber Command publicly speculated that ransomware attacks have been used by states as a cover to test the utility of hacking tools against hospitals and energy infrastructure.[5]

2.2.2 NEW EVIDENCE FROM THE WAR AGAINST UKRAINE

While this might be an instance of worst-case thinking, the tendency to mask political attacks as criminal operations is real and will likely become more widespread.[6] In the run-up to the Russian invasion of Ukraine, at least one of the wipers used to attack Ukrainian governmental organisations and businesses was disguised as ransomware (Greig 2022). Later, in November 2022, Microsoft researchers attributed a ransomware campaign against transportation and related logistics industries in Ukraine and Poland to Sandworm, a Russian military intelligence group (Microsoft 2022). Yet another ransomware attack on Ukrainian organisations was also attributed to Sandworm by ESET researchers (Paganini 2022). It is also conceivable that Russia will at some point emulate the North Korean practice of evading international sanctions through state-led cybercrime operations (Schwartz 2022; Blachmann 2021; Brady and Heinl 2020: 45). The regime of Kim Jong-Un has reportedly raised two billion US dollars to fund its weapons programmes by conducting cyberattacks against banks and cryptocurrencies exchanges in 17 countries according to a 2019 report presented to the UN Security Council Sanctions Committee on North Korea. In addition, cyberspace was used for money laundering purposes by North Korean groups (Nichols 2019). More recent studies estimate that North Korean hackers have been able to steal between 600 million and one billion US dollars in cryptocurrencies in 2022 alone (Nichols 2023). Another report published byUS and South Korean intelligence services puts special emphasis on North Korean ransomware attacks against critical healthcare facilities (United States National Security Agency et al. 2023). Iran is another 'pariah regime' suspected of sponsoring financially motivated cybercrime (Microsoft 2021).

Even if Russia does not follow the North Korean example, its war of aggression against Ukraine may nonetheless have a lasting impact on the cybercrime ecology by politicising and splitting cybercriminals in Russia and other countries apart (Microsoft 2023: 42–43; Accenture 2022; Uren 2022). Thus Conti, one of the largest ransomware groups declared its "full support" for the Russian government and threatened to use "all possible resources to strike back at the critical infrastructures" of its enemies merely one day after the Russian invasion (Bing 2022).[7] Stormous, another notorious group, issued a similar warning particularly to France.[8] Other groups, such as LockBit, declared themselves neutral while referencing the diverse citizenships of its members (Pearson and

Satter 2022). Overall, it is difficult to assess the degree to which cybercriminal groups have played an active part in the war. The vast majority of Russian attacks on Ukrainian infrastructure and data networks during the invasion seem to be conducted by state intelligence services rather than by criminal cyber proxies (Nichols 2022; Bateman 2022: 36). According to a first systematic study, the role of the cybercriminal underground "in the conflict appears to have been minor and short-lived" (Vu et al. 2022). It is worth mentioning that this study was limited to a quantitative analysis of website defacements and DDoS-attacks without including more sophisticated cyber intrusions like destructive ransomware attacks or hack and leak operations.

Focussing on the latter, there is at least some anecdotal evidence of criminal operations in support of the Russian war effort (Antoniuk 2023; Microsoft 2023: 44–45). The TrickBot operation, for example, that was subsumed by Conti towards the end of 2021,[9] was involved in six campaigns against Ukrainian targets from the start of the Russian invasion to July 2022, according to IBM's Security X-Force (Villadsen 2022; Holdemann 2022). If true, this would signal a growing interest in Russian war aims and a clear break-away from past business practices not to attack targets within former Soviet Union territories (Grünewald 2022).[10] The findings of IBM's threat intelligence team are corroborated by Google researchers who see recent TrickBot/Conti operations against Ukrainian targets as "representative examples of blurring lines between financially motivated and government-backed groups in Eastern Europe, illustrating a trend of threat actors changing their targeting to align with regional geopolitical interests" (Bureau 2022). Another example of this tendency is the use of RomCom, a tool developed by the Cuba ransomware group, against users of the Ukrainian DELTA military system (Microsoft 2023: 44). The case of Killnet deserves special attention as well. Starting as a hack-for-hire-vendor in January 2022, it transformed into a donation-funded political hacker collective soon after the Russian invasion of Ukraine, claiming responsibility for several DDoS-attacks against NATO countries (Smith et al. 2022; Antoniuk 2023). While being rather unsophisticated from a technical perspective, some of these attacks reportedly made US health care facilities take down IT systems and suspend medical services. It has also been reported that Passion group, a Killnet affiliate, began offering DDoS-as-a-Service to various pro-Russian hacktivists who intended to target North American and European hospitals (The CyberWire 2023).

Other cybercrime actors, while not shifting their primary identity like Killnet, at least seem to have changed their code of conduct towards fellow criminals within the criminal ecosystem. For example, it is reported that some network access brokers have decided to exclusively sell to pro-Russian sources or to offer special discounts to them, while declining to sell access to groups who aim at targeting Russian entities (Vicens 2022). Another notable change has been calls to let ransomware groups return to mainstream underground forums from which they had been banned in the aftermath of the 2021 Colonial Pipeline attack[11], obviously to pre-empt increased scrutiny from law enforcement (Accenture 2022: 3–4). In other cases, efforts have been made to ban Russian users from criminal fora. In the case of RaidForum, such an announcement apparently led to the seizure of the forum by an unknown party on the very same day (Ilascu 2022a; Flashpoint 2022). Rising numbers of ransomware attacks against Russian institutions in the first quarter of 2022 (ESET 2022: 19) could also reflect structural changes as these violate the informal codex of not provoking the Kremlin or affiliated regimes. In a survey conducted on the Russian language XSS cybercrime forum, 17% said they were willing to target Russian entities (Accenture 2022: 1). In one notable incident, hackers used Conti's leaked ransomware source code to target Russian businesses and organisations, leaving a note saying "Your President should not have committed war crimes. If you're searching for someone to blame for your current situation look no further than Vladimir Putin" (quoted in Abrams 2022a). Researchers have also discovered a pro-Ukraine cybercriminal forum, dubbed Dumps, that explicitly only allows targeting victims in Russia and Belarus (Scroxton 2022). Again, it is too early to say whether such instances reflect long-term structural shifts or merely episodes.[12] Publicly available data also does not make it possible to assess the seriousness of some of the claims made by criminal groups, nor is it possible to conclusively rate the success of politically driven cyber operations of various non-state actors.

2.2.3 GLOBAL RAMIFICATIONS

These caveats aside, a lasting politicisation of cybercrime and/or additional ways of instrumentalisation by state agencies would certainly have a negative impact on international crisis management and conflict prevention. First, the use of criminal proxies facilitates violations of the UN norms of responsible state behaviour by offering plausible deniability. Not tackling cybercrime therefore runs counter to one of the core stabilisation mechanisms as developed and confirmed by the

UN GGE and the UN OEWG (see United Nations General Assembly 2021; Group of Governmental Experts 2021). Second, synergies and operational merging between cybercrime and political sabotage will make it even harder to separate the roles of the military, intelligence, and law enforcement services in responding to cyberattacks (Brady and Heinl 2020: 44). This, in turn, could lead to the ineffectiveness of established trans-governmental communication channels and similar confidence-building measures, especially when cross-border investigations or disruptive attacks against criminal infrastructures are conducted without the knowledge of other state security agencies. It could also lead to overreactions of state sponsors of cybercrime or third parties if network intrusions are traced back to military units instead of law enforcement agencies.

For all of these reasons, there is thus a growing need to effectively curb cybercrime through international cooperation. For example, the global network of governmental single-points-of-contacts (PoCs), envisaged as a key confidence-building measure by numerous UN member states, could facilitate the clarification of such misunderstandings but is certainly not enough (Australia et al. 2022). More generally, scholars have pointed out the need to establish stronger links between cybercrime discussions within the UNGA's Third Committee and cybersecurity debates within the OEWG (located in UNGA's First Committee) (see, for example, Hakmeh and Vignard 2021: 25–26; Swali and Naylor 2021; Peters and Garcia 2020: 49). The aim would be not only to coordinate agenda items but also, through consultation with UN bodies and expert communities, to ensure that institutional solutions reinforce the aims of both regulation areas. Amongst other things, this may lead to a greater emphasis on institutions that promise to offer benefits for both cyber crisis management and international cooperation against cybercrime. A case in point would be the recognition of common attribution standards (Shany and Schmitt 2020; Droz and Stauffacher 2018; David II et al. 2017; Charney et al. 2016: 11–12). Such recognitions could also be combined with multilateral adjudication processes, as pointed out by Healy et al. (2014: 10–12).

Another institutional remedy could be an independent repository of data requests. This might not only help assess the practical usefulness or deficits of law enforcement cooperation mechanisms. But it would also, ideally, highlight uncooperative behaviour, for example, the practice of refusing to participate in the investigation of cyberattacks (provided there is an adequate and impartial classification scheme). At the same time, proven compliance and support of

investigations would act as a reassurance mechanism with stabilising effects well beyond the narrow area of collaboration against cybercrime. To have any deterrent effect on private hackers, however, such mechanisms would require international consensus on state due diligence for policing such actors (Healy et al. 2014: 11); a principle that is currently still very much disputed (Mikanagi 2021; Patrick 2019; Schmitt 2015). There is also the risk of bogus requests and other blame shifting tactics that could well undermine such accountability mechanisms. In line with this idea (although certainly further down the road) are additional suggestions to use international criminal law as a deterrence against particular harmful actions in cyberspace, independent of criminal or political driving motives behind them. While the International Criminal Court (ICC) seems ill-suited to handle transnational cyber offences[13], a specialised criminal court could be established to deter grave cyber offences and to put additional pressure on uncooperative governments. Kraft and Streit (2011), as well as Schjolberg (2012), have published proposals for such an International Court for Cybercrime or an International Criminal Tribunal for Cyberspace. The litmus test for any such institution would, of course, be its ability to deter future cybercrime of the sorts seen during recent large-scale ransomware attacks.

2.3 FROM PRIVATE DEFENCE TO CYBER VIGILANTISM

The literature on state failure explains that an erosion of basic public goods provision, with citizens left to their own devices to escape violence or starvation, creates opportunities for war lords and other political entrepreneurs to offer protection in exchange for private 'taxes' and political loyalty (Thomas et al. 2005: 55–57). Another possibility is the development of an anarchic self-help system with high levels of insecurity and violence. In either case, the system succeeding a state monopoly of violence has inbuilt tendencies to sustain high levels of insecurity, making the reinstitution of democratic accountability increasingly challenging. With a burgeoning cybercrime market and insufficient international cooperation against cybercrime, similar risks could materialise in cyberspace.

For more than a decade, business operatives and strategists have made the case for public authorities to condone or even explicitly legitimise private hack-backs in cyberspace. Such measures could be limited to intelligence collection within

the networks of attackers, or they could actively seek to disrupt or degrade adversarial infrastructures. Almost every major cybercrime incident has given new impetus to this debate (Townsend 2021; Robertson and Riley 2014; Williams 2021; Soesanto 2021). While the practice of hacking into adversarial systems, or mere stepping stones, is arguably an open secret in some business sectors (Schmidle 2018; Cox 2017),[14] domestic laws in most countries do not permit such actions, at least not explicitly (see Housen-Couriel 2020: 112–116; also see Corcoran 2020 for a discussion of few exceptions). Legalisation would therefore create a new situation, with fewer business operatives being deterred from hack-backs by serious liability risks. There is already a market for commercial active defence services, with companies being ready to expand their business models following legislative changes.

While the majority of counterarguments against private hack-backs tend to focus on their domestic repercussions – from possible interference with legitimate law enforcement operations to an erosion of democratic accountability – it bears mentioning that one of the emerging features of this private self-help system would be its transnational nature. Even if most states decide not to legalise private hack-backs, the outcome might look very similar since offshore companies or jurisdiction shopping make it possible to evade national laws (Hoffmann and Nyikos 2018: 6, 10). Further underlining the transnational nature of the problem, there is an increased risk of unintended cross-border escalation due to misperception of the intent and origin of private hack-backs. Competition between active defence service providers will, again, add to the picture. More specifically, the need to offer competitive prices combined with the shortage of skilled labour calls into question the ability of commercial hack-back providers to minimise collateral damage and to avoid transnational escalation. This will, in turn, add to the aforementioned peace and security risks.

One way to avoid a full-blown privatisation or outsourcing of active cyber defence would of course be effective governmental action. Yet because of the truly transnational nature of cybercrime, unilateral responses are oftentimes insufficient and/or they increase international tensions. This can already be seen with the extraterritorial effects of cybercrime legislation (Internet Society 2018). It becomes even more controversial with cross-border law enforcement or even military counter-crime operations. Simply put, any network intrusion could, in theory, be misused for purposes beyond defensive measures. Here, again, the risks of misperception and the possibility of unwanted escalation are obvious.

The expected security benefit must be balanced against the international political 'fallout' of such operations. Any unilateral operation may also endanger the success of parallel private or multilateral coalition action. The US Cyber Command's take-down of the TrickBot network in 2020, which apparently was uncoordinated with the actions of a Microsoft-led global coalition, is a case in point (Healy 2021).[15] On the other hand, there is remarkably little public criticism of such operations from NATO members and other US allies so far, a tendency that could well signal a tacit normalisation of such practices.

Other proposals seek a closer integration of internet service providers, hardware vendors or cybersecurity companies in existing law enforcement approaches (Boes and Leukfeldt 2017: 186–187). Not only do they have unique visibility into supply chain vulnerabilities and interdependencies, global internet traffic, and sophisticated technical skills but they often also have more opportunities to analyse and dismantle cyber infrastructures and assets that criminals use (Zettl-Schabath 2022; World Economic Forum 2020: 18). It is therefore unsurprising that victim organisations turn to private contractors for recovery and investigation rather than contacting law enforcement (World Economic Forum 2020: 11). Yet instead of discouraging victim organisations from doing so, law enforcement agencies would perhaps be better advised to pool resources with companies (World Economic Forum 2020: 12; see also European Commission 2015: 20). The core aim would essentially be to mutually support each other's mission, i.e., leveraging private-sector investigations for enforcement activities and enhancing recovery and continuity of business-efforts by capitalising on law enforcement insights. As within other internet-related policy areas, for example online content moderation within Europe, such arrangements would move beyond conventional Public-Private-Partnerships and towards the "co-production of security decisions" (Bellanova and de Goede 2021: 1320; see also Nolte and Westermeier 2020).

Existing cooperation platforms such as the Cyber Threat Alliance (CTA) or Interpol's Project Gateway exemplify such ambitions beyond the national level. Yet there are many challenges, ranging from clear divisions of responsibilities to making sure that disclosed evidence meets judiciary standards (Boes and Leukfeldt 2017: 193–194; Eurojust 2022: 22). Cooperating partners also need to respect security concerns and legal obligations of individual partners, for example privacy regulations that restrict the sharing of customer data (Walker 2019: 8). A promising way to maximise benefits of cooperation without violating privacy

regulations is the use of masked federated learning, homomorphic encryption, and other innovative technologies that enable individual partners to process queries on each other's data without actually being able to know what the other's data is (World Economic Forum 2020: 14; ENISA 2021; Schallbruch et al. 2021).

Sometimes the most promising way to deal with cybercrime is not to investigate and prosecute individuals but to disrupt cybercriminal ecosystems, for example by seizing accounts and restricting revenue streams or by disabling technical infrastructures (World Economic Forum 2020: 18; Zettl-Schabath 2022). Disabling of the GameOver Zeus botnet in 2014 or the FBI-led global coalition against 3ve, an enormous ad fraud botnet in 2018, exemplify the potential of pooling public and private resources to this aim (US Department of Justice 2018b). In another remarkable case, in January 2021, law enforcement agencies from eight countries coordinated with private security researchers to take down Emotet, another notorious cybercrime infrastructure (Manky 2021), though it has resurfaced in modified form since. While sceptics doubt any sustainable effects of such operations given that criminal infrastructures often quickly recover or reappear in different shapes, disrupting ongoing criminal campaigns nonetheless reduces immediate dangers. Demonstrable benefits of such partnerships are key to convincing victim organisations of refraining from unilateral active defence measures, a major (if not the single most important) policy aim from a peace and security perspective.

At the same time there are still obvious concerns about unintended consequences and escalation spirals. At a minimum, there is a need to establish legal authority and accountability for disruptive operations, by ensuring that at least one cooperating partner is responsible and legally permitted to take actions under national and international law (World Economic Forum 2020: 19). Furthermore, coalition partners should carefully consider unintended consequences as well as the perceived legitimacy of disruptive operations by third parties. Recent proposals to establish operational guidelines for "responsible cyber offense" (Adams et al. 2021) may serve as a useful framework in this regard, emphasising and specifying ways of limiting collateral damage, constraining automation, and preventing third-party access to backdoors and other attacking tools. If such safeguards and guidelines will suffice to essentially replace private hack backs with legal and more legitimate hybrid alternatives remains to be seen. On the other hand, there is a counterfactual risk of banning private hack-backs without

offering an alternative. This may be counterproductive by forcing an established practice to remain hidden from public authorities, leaving the latter unable to anticipate or mitigate international escalation risks.

2.4 MISUSE, DOMESTIC STABILITY, AND RULE OF LAW

Finally, while multilateral collaboration is vital as seen above, it needs to be carefully designed to avoid indirect peace and security risks due to governmental abuse. There already is a growing trend of authoritarian and semi-authoritarian countries using cybercrime legislation as a pretext for cracking down on human rights and individual freedoms, as seen in the MENA-region (Ben-Hassine and Samaro 2019; Gulf Centre for Human Rights 2018) or Western Africa (Global Initiative against Transnational Crime 2022). "Weaponization of cybercrime" as Rodriguez and Baghdasaryan (2022) put it, is widely used to target journalists, whistle-blowers, political dissidents, security researchers, LGBTQ communities, and human rights defenders. Vague international obligations to criminalise and prosecute cybercrimes may well add further legitimacy to such policies.[16] Domestic repression could, in extreme cases, tip the scale towards violent resistance and civil war. Political science studies indicate that mixed regime types or transitional societies, where there is at least some political competition but also weak institutions, are more prone to violent conflict than either full-blown autocracies or stable democracies (Mansfield and Snyder 2005; Gleditsch and Ruggeri 2010). In other words: it is precisely in this context of limited political competition where it is crucial to be able to influence the decision calculus of incumbent leaders in order to prevent violence and destabilisation. Ill-defined international obligations to tackle cybercrime could help these leaders to diffuse international opposition and thus to escape external pressures. Inasmuch as this is the case, the design of international agreements on cybercrime can possibly have real, albeit indirect and limited effects on the probability of violence in fragile world regions.[17]

This is not to say that international or regional cooperation against cybercrime is or likely will be a key enabling factor of political violence in many cases. Yet the potential for misuse cannot be denied and must be addressed by appropriate safeguards. Article 15 of the Budapest Convention of the Council of Europe[18],

the currently only truly interregional and legally binding agreement[19] in this policy area, explicitly provides that each party shall ensure that the implementation and application of the Convention is subject to the safeguards provided under its domestic law and international human rights treaties. The Convention also does not prevent member states from submitting to stricter privacy standards, as can be found in the Council of Europe's Data Protection Convention (Council of Europe 2018) or the General Data Protection Regulation of the European Union (2016). While these provisions and safeguards clearly limit the potential for misuse, privacy activists and data protection experts continue to have concerns regarding some of the provisions, both in the original Convention and in the draft second additional protocol. For instance, objections were raised against the scope of subscriber information and the possibility of sidelining independent judicial authorities during transnational data disclosures (Asociación por los Derechos Civiles 2021; Office of the Privacy Commissioner of Canada 2021; Council of Europe 2021; Rodriguez 2017). Similar criticism has also been directed against the so-called e-Evidence Package, i.e., proposals by the European Commission and the European Council on facilitated cross-border access to electronic evidence within the European Union (Wahl 2020, 2021; Carrera et al. 2020: 55–58).[20] Recent reports also highlight the risk of fake emergency data requests used by cybercriminals to obtain addresses, phone numbers, and other sensitive information from Apple and Meta (Hardcastle 2022).

While these are of course legitimate concerns, the start of negotiations on a new universal cybercrime treaty within the UN Ad Hoc Committee, initiated by Russia, led to far greater worries about risks to privacy and human rights protections (Knodel 2022). Promoting an alternative model to the Budapest Convention, Russia submitted a draft treaty titled "United Nations Convention on Countering the Use of Information and Communications Technologies for Criminal Purposes" (see unofficial translation by Kommersant 2021) already prior to the start of negotiations. Within this draft treaty, the language on what constitutes the use of communication and information technologies (ICTs) for criminal purposes is extremely vague, causing "overreach in criminalization" (Hakmeh and Tropina 2021). For example, the scope of the Articles 20 and 21 on "terrorism-related offenses" and "extremism-related offenses", respectively, is very broad and does not offer any safeguards against domestic misuse. Technical terms such as "malicious software" (Article 4c, Article 10) are similarly vague and could, theoretically, be used to criminalise, for example, the circumvention of national firewalls via Virtual Private Networks (VPN) or other tools. Furthermore

and with regard to procedural issues, the draft "lacks the precision and distinction available in existing instruments" (Hakmeh and Tropina 2021), thus complicating the application of safeguards.

Russia's agenda setting power suffered a major blow right at the beginning of UN negotiations due to its war of aggression against Ukraine. Yet other authoritarian states pushed for similar policy agendas. Their influence within the negotiations is testified by some provisions within the so-called Consolidated Negotiation Document (CND) that was presented by the Chairwoman of the UN Ad Hoc Committee in the run-up to the second round of negotiations starting in January 2023 (United Nations 2022). For example, the draft still criminalizes "extremism-related offences" (Article 27) and vaguely refers to activities such as "the spreading of strife, sedition, hatred or racism" via ICTs, as lamented by numerous human rights organisations in a letter to the Committee (Electronic Frontier Foundation et al. 2023).

As mentioned earlier, authoritarian governments may well use permissive norms and ambivalent vague definitions within a new cybercrime treaty as a cover for intimidating and prosecuting non-violent political opponents. It would not be the first case in which authoritarian governments copy and misuse policy instruments from other contexts. A case in point might be Germany's Netzwerkdurchsetzungsgesetz (Network Enforcement Law) against online hate speech. Some argue that this law has been used as a template by several non-democratic countries to crack down on dissidents (Mchangama and Fiss 2019). An ill-devised UN treaty without effective human rights and data protection safeguards could be used to criminalise and supress critical online content, and to pressure internet and social media companies into cooperating with data requests. Against this backdrop, it is of paramount importance that any global treaty on cybercrime is both limited in scope (avoiding overreach in criminalisation) and that it does not undermine or circumvent effective privacy and other human rights standards. Absent of global standards of data protection, international cooperation procedures must default to the highest standard between parties. Furthermore, expedited cooperation in urgent circumstances should not allow skirting due process and judicial review (Knodel 2022).

That having been said, gaps and loopholes in the international harmonisation of cybercrime can be just as worrying as the potential for misuse. Recent revelations of commercially available spyware being used by numerous countries are

a stark reminder in this regard (Kirchgaessner et al. 2021). So far, business leaders face virtually no consequences for evading export regulations, leading some observers to claim that the global spyware industry is "totally out of control" (Ropek 2021). The 2021 indictment of the former leaders of Amesys, a French surveillance company, for selling equipment to Egypt and Libya and thereby facilitating the torturing and disappearing of dissidents, has been a notable but rare exception (O'Neill 2021b). An international commitment to consequently prosecute acts of export control evasion and international obligations to assist with the investigations of suspected business leaders could be one significant safeguard, alongside more restrictive export control policies themselves.[21] Furthermore, international policy deliberations and norm-building efforts must pay greater attention to the criminal activities of governmental actors themselves. This includes worrying new ways of collaborating with private hackers in the fabrication of digital evidence against dissidents (Greenberg 2022).

As argued before, ambiguities and unpredictable effects of cybercrime pose challenges to the separation of powers and security agency mandates also in democracies. One aspect relates to the boundaries between domestic law enforcement, intelligence services, and the military. In the United States, for example, calls for cutting red tape and military Cyber Command take-over are increasing (Van de Velde 2022 is a case in point, see also the argument between Healy 2021 and Pascucci and Sanger 2021). The US Cyber Command explicitly confirmed it would take an active role in combatting ransomware (CNN 2021), as did the UK GCHQ (Warrell 2021). Yet any operational role of the military or intelligence services in the fight against cybercrime could have political downsides. Due to these institutions' offensive mission, it will probably increase international mistrust and offer the perfect excuse for countries who do not want to cooperate against state affiliated cybercrime actors.

In the long run, systematic reliance on military organisational and technical capacities could possibly 'spill-over' in other policy-areas as well, especially in unconsolidated political regimes. Any such development would run counter to international efforts to curb the role of the military and to establish checks and balances on state executives in fragile societies and war-torn regions. In other words: there is a clear contradiction between blurring military, intelligence, and police responsibilities at home while at the same time advocating functional differentiation between military, paramilitary, and police forces abroad, the latter being a traditional core aim of security sector reform (see Brzoska 2000: 10).

International capacity-building efforts in the area of cybercrime are already fraught with tensions between the need to support an effective global law enforcement regime and the risk of misuse for political repression.

At least at the national, and possibly even at the international level, state parties should therefore commit themselves to establishing and sustaining effective monitoring and review mechanisms to make sure that cyber capacity building does not have unintended effects on broader foreign policy objectives such as securing a free internet (Peters and Garcia 2020: 54). Within the US government itself, periodic compliance reviews are used as an instrument to make sure there is no data access misuse.[22] Similar policies might be developed and coordinated among other democratic countries, thus creating a coherent and effective lever to avoid the instrumentalisation of law enforcement cooperation for violent regime survival strategies. To avoid allegations of hypocrisy, democratic states themselves could do more to document the application of safeguards to their own data collection. One possible option could be to aim for a public repository within an independent body that provides some basic information on the scope and nature of particular cross-border searches, including the application of legal safeguards (Koops and Goodwin 2014: 6). Furthermore, the 2017 Council of Europe report on best practices of generating and providing statistics on the effectiveness of MLATs by member states could be used as another starting point for reviewing workable mechanisms (Council of Europe 2017: 8). Finally, preparatory work for the second additional Protocol (T-CY Cloud Evidence Group) had made ample use of data published by service providers in their voluntary transparency reports. However, service providers were not required to issue such reports in the future, a regulatory effort that would significantly improve the reliability of any aggregated data assessment.

3 The Need for an Integrated Perspective

Thus far, one of our key arguments has been that the uncertainty surrounding actor behaviour and their intentions greatly complicates effective and legitimate policy responses, particularly in regard to peace and security implications of cybercrime. Independent research could play a major role in reducing such uncertainties and as a facilitator of evidence-based policy-making at the national and international levels. However, one of the key impediments – beyond data availability – is the interdisciplinary nature of this topic, with traditional boundaries preventing researchers gaining a comprehensive understanding of cybercrime, including technical, legal, and social aspects. We therefore argue that an integrated perspective, combining different and dispersed silos of knowledge as well as research methodologies, is needed to answer some of the most pressing questions in this policy area. Such open questions both relate to causal impact of cybercrime and to the effectiveness or side-effects of institutional mechanisms to deal with it.

Understanding the factors that strengthen or erode escalation control is one obvious area. Here insights from computer science on the technical characteristics of criminal command & control infrastructure need to be combined with sociological surveys on criminal operator attitudes and values in order to gain a clearer understanding of the factors that may or may not lead to risk-taking behaviours. Some recent studies for example have questioned the dominant rational choice framework for understanding and preventing cybercriminal behaviour by emphasising the importance of emotional factors such as frustration and boredom (Collier et al. 2020). Such factors also need to be taken into account while assessing the benefits or risks of disrupting criminal infrastructures. For example, in some cases, crackdowns on criminal infrastructures could backfire by uniting criminal online communities against a ‘common enemy’, a strength that could easily outweigh any loss in tactical operational capacities (Ladegard 2019). The recent Conti leaks offer a treasure trove for such sociological studies.

At the same time, we need a better understanding of the perception of criminal cyber operations by victim organisations, political elites, and the public in order to assess likely spill-overs into international political escalation. Systematic studies on these topics have only begun to emerge (Gomez 2021). Finally, there

is the question of what the long-term effects of an increasingly militarised approach towards cybercrime in some countries will be. This requires greater and more systematic data collection about civil-military institutional relationships, as well as military norms and values in this particular area. So far, such studies have almost exclusively focussed on constitutional issues that arise from delegated authority within the United States (Healey 2022; Rudesill 2020; Jensen and Work 2018). Yet, such challenges might look rather different within a European parliamentary system and even more so within less consolidated democracies that are in the midst of a political transition from or to semi-authoritarian rule.

Lack of knowledge about the mobility of 'criminal labour' (see for example Kaspersky 2022) is arguably another major impediment to understanding the nexus between peace and cybercrime. Discussions about unintended side-effects of unilateral actions against transnational crime have long centred on a so-called balloon effect (Windle and Farrell 2012). The latter describes the phenomenon that successes for example in the fight against drug trafficking in a particular regional area do not necessarily result in an overall reduction of the profitability of such criminal businesses. Rather they may simply cause a diversion of criminal activity to other regions or sectors where there is less prosecution pressure. Similar effects very likely characterise the global cybercrime ecology. The fact that the US President elevated the fight against ransomware to a national security priority in 2021, combined with the heightened alertness towards any malicious cyber activity from Russia in the context of the invasion of Ukraine, may well have contributed to a significant drop of ransomware attacks against US targets. The US share of global ransomware victim organisations indeed fell from 54% in the first five months of 2021 to 38.5% in 2022, according to Allan Liska from Recorded Future. Among the potential reasons he indicated is the possibility that ransomware groups deliberately chose not to put US companies on their extortion site list (Doyle 2022).[23] At the same time, the global ransomware business in 2022 seems to be only slightly less active than in the year before according to the number of detected attacks (ESET 2022). In line with this pattern, cybersecurity researchers and industry professionals report a rising share of criminal cyber operations against companies and public institutions in mid-income as well as developing countries within the Global South (Delcker 2022). This trend is expected to continue due to widening protection gaps, according to insurance company Moody's (Kapko 2022).[24]

Gauging the extent of such balloon effects more systematically within the regional and global cybercrime market and moving beyond mere description to explanation / prediction would again require a mixture of disciplinary and methodological approaches, ranging from computer science to sociology to economics. A similar question might be raised with regard to the fluidity of 'criminal labour' between cybercrime and other 'analogous' crimes. While there is an ongoing discussion within international security studies about the relative utility of cyber operations versus kinetic violence in the context of the current war in Eastern Europe (Maschmeyer and Kostyuk 2022), far less is known about the inclination of cybercriminals to switch to other businesses, both legal and illegal, if the former becomes less profitable. Also, the perception of cybercrime as perhaps less peace-threatening than physical crimes might change in the future, with the growing disruption caused by criminal attacks on critical infrastructures.

Finally, perceived risks of the abuse of international agreements in the domestic policy area need to be substantiated by empirical evidence – or disproved. The aim here is not to debunk the existence of such risks but to find ways to avoid such unintended effects of international regulation. One way to do so is to combine technical and legal analysis of ambiguities and loopholes with conceptual and empirical norm research within the social sciences. For example, the latter could systematically assess the role of international commitments within authoritarian state justifications for repressive laws and practices. Technical and legal experts on the other hand could weigh indicators of fabricated evidence and other abuses, comparing the actual behaviour of regime member states to non-members. Social scientists, in turn, could focus on the salience and framing of such abuses within media reporting, again seeking to identify and explain differences between states within or without international cooperation agreements. The results of such comparisons would ideally help to assess the real risk of 'unintended legitimisation' cases.

4 Conclusion

Cybercrime and the fight against it are no longer a niche topic: the economic repercussions alone are too high. Other costs, however, such as the social and political issues that can aggravate domestic instability or even fan international crises, are rarely at the forefront of discussions. The goal of this study has been to systematically explore such missing links and to emphasise the way in which global cybercrime already does – or in the future plausibly could – affect peace and security both within and between societies. Our focus has been predominately on cyber-dependent crimes, as their characteristics limit the applicability of existing public policy and international security templates.

As far as intra-societal peace is concerned, the available evidence first and foremost requires us to abandon the idea of cybercrime as a geographical one-way street, with criminal perpetrators acting out of poor countries against targets within wealthy states. In fact, the growth rates for example of ransomware or DDoS attacks in some regions within the Global South are higher than in many European or North American countries. Cybercrime is 'catching up' while at the same time having regional characteristics. Moreover, the victims of cybercrime also include public schools, medial services and local administration, thus disproportionally affecting the more vulnerable parts of society. Extrapolating from the current growth rates in fragile world regions there is thus a significant risk that cybercrime will aggravate existing distributional conflicts. It already seems plausible that cybercrime increasingly fuels war economies, provides an avenue for financing weapons, destabilises societies through the spread of disinformation, and provides a means of undermining international sanctions. International cooperation would be beneficial in many cases, yet other basic elements are lacking, such as for example comprehensive national cybersecurity strategies or additional resources to implement these.

Criminal cyber operations can also threaten peace at the global level due to the shared use of TTPs with other actors, or even actors having several agendas (Sadowski 2023). While cybercrime is predominantly driven by financial motivations, this aspect can be difficult to ascertain, particularly in early stages of a system compromise. This issue is further aggravated by sophisticated threat actors, who may be linked to various governments, but often overlap with the cybercriminal eco system, which has already developed complex hiring processes and labour division. Another example is the potential of criminal cyberattacks

and private counterattacks being misinterpreted as state operations, especially in a climate of increasing geopolitical tensions. Coupled with the issue of cyber-attacks hitting the 'wrong' target or causing collateral damage an argument can be made that the risk of misinterpretation and unintended escalation increases greatly. In the wake of Russia's war of aggression against Ukraine, the politicisation of the criminal underground has intensified, especially in Eastern Europe, amplifying the challenge of differentiating between state and non-state actors. To avoid unintended escalations, states must establish and apply crisis management mechanisms while at the same time increase the pressure against those who support or instrumentalise cybercrime.

Unsurprisingly, hack-backs and cyber vigilantism have again been invoked as a possible solution, particularly given the expertise and resources held by private entities. While there have been success stories in private-public takedowns of malicious networks and operations, legal authorities and accountabilities for disruptive operations are sometimes unclear and could thus add to an international climate of mistrust and worst-case thinking. Furthermore, unintended consequences and possible escalatory spirals are also of concern, as third parties could challenge the perceived legitimacy of disruptive operations. Similar risks relate to unilateral military responses, for example to ransomware operations.

Strengthening international cooperation against cybercrime should therefore be favoured over unilateral or private responses, particularly from a peace studies perspective. However, it is important not to legitimise excessive uses of state power or allow ambiguity that could lead to misuse. Journalists and human rights activists have already reported numerous cases in which cybercrime legislation has been misused against political dissidents, particularly from within authoritarian countries. Likewise, a cautious approach is needed with regard to international capacity-building that includes non-democratic recipient countries. Here, there is a risk of unintendedly supporting unaccountable or even repressive security agencies.

Such potentially negative human rights impacts also need to be taken into account when assessing the current negotiations on a convention against cybercrime at the UN. On the one hand, the envisaged convention, being the first universal instrument of its kind, could expand the circle of cooperating states and impede the jurisdiction hopping of cybercriminals. For example, homogeneous definitions of criminal offences as well as simplified and accelerated process-

es for data exchange could contribute to this. The expansion of technical and administrative assistance for weaker states also plays a role in the negotiations. Nevertheless, an interim assessment from the perspective of peace studies is ambivalent. It is no coincidence that the initiative for a UN convention came from Russia and other authoritarian states. One presumed impetus was the weakening of existing cooperation mechanisms, especially the Council of Europe's Convention on Cybercrime. Another could be authoritarian states seeking to legitimise excessive powers and repressive practices by security agencies. In this context, it cannot be stressed enough that the principles defined in the Convention concern far more than 'just' cybersecurity policy, for example in the storage and interstate exchange of digital evidence. After all, almost every offence nowadays leaves digital traces. It is therefore all the more important that human rights obligations and procedural standards based on the rule of law are enshrined in the draft treaty. In addition, it must be a matter of ensuring compatibility with the existing Budapest Convention against Computer Crime. Only if these preconditions are met can the convention as a whole make a contribution to peace inside and outside of cyberspace instead of itself becoming – even if only indirectly – a risk to peace.

Endnotes

1 The official title of the committee is Ad Hoc Committee to Elaborate a Comprehensive International Convention on Countering the Use of Information and Communications Technologies for Criminal Purposes.

2 In the cybersecurity community, TTPs – tactics, techniques, and procedures – refer to the behaviour of a threat actor when conducting cyberattacks. More specifically, they describe an actor's processes and actions at various levels, with tactics forming the top 'layer'. It essentially is the overall goal or overarching plan, such as for example wanting to exploit a website in order to gain access to customer payment information. The middle layer are the techniques that are employed to reach said goal, which in the example above could be cross-site scripting, injection attacks, or other methods. The procedures are the lowest and most detailed level, including a highly comprehensive description of behaviour and a step-by-step analysis of the attack, which in turn also provides the most information about the perpetrator. TTPs can, for example, help draw conclusions about the attack framework and thus contribute to incident response, risk assessments, and threat mitigation. Moreover, they can be used for threat modelling or intelligence sharing, particularly when the same attack is being tracked and analysed by different security researchers or companies. For more information, see for example https://azeria-labs.com/tactics-techniques-and-procedures-ttps/ (accessed 24 March 2023).

3 See Dark Web Prince Index 2022 at https://www.privacyaffairs.com/dark-web-price-index-2022/ (accessed 21 June 2022).

4 Also in 2022, a threat actor, most likely from Iran, used ransomware against Albanian governmental institutions ahead of an Iranian opposition conference in the Southeast-European country. The Albanian government responded in an unprecedented way by cutting all diplomatic ties to Iran. The initial cyberattack was coercive in nature, however. Therefore ransomware was not used as a cover but to deliver a political message, also including an explicit political warning as part of the ransom note (Jenkins et al. 2022).

5 See comments by Didier Tisseyre, head of Cyber Defence Command (COMCYBER) of the French armed forces on twitter (https://twitter.com/ComcyberFR/status/1412309720904392710, accessed 6 August 2021): "Ce que je vois derrière cette cybercriminalité, ce sont certains Etats qui sont en train de se positionner. Ils testent leurs outils, sur les hôpitaux ou dans le secteur de l'énergie notamment"

6 False flags and similar techniques are not a one way street however, Some criminal groups, for example, claim to be associated with well-known state-affiliated actors in order to scare their victims into paying the ransom (Europol 2021: 23).

7 Conti itself quickly offered a second statement somewhat inconsistent with the first one, saying that it actually opposed the war while still blaming and threatening the West and NATO (Pearson and Satter 2022). This change might have resulted from the fear of retaliatory actions by non-Russian insiders, given that the group includes Ukrainian nationals. In fact, the group suffered from a major data leak soon after the episode, although the data was leaked by a Ukrainian security researcher who had gained access to the criminal infrastructure rather than from an insider. Others have pointed out that financial incentives work against a stronger politicization of cybercrime, given that cyber insurances do not necessarily cover costs due to politically motivated cyberattacks (Weber 2022). Without such coverage however, victim organisations are likely to pay less ransom to attackers, causing criminal profit rates to drop.

8 See tweet from DarkTracer https://twitter.com/darktracer_int/status/1511110352775254018 (accessed 16th June 2022).

9 TrickBot is a malware platform focused on Windows systems and it uses different modules for various malicious activity. For example, some are centred on stealing passwords or information, while others deliver additional malware or provided network access. It dominated the market since 2016, collaborating with ransomware groups and affecting millions of devices globally. Surviving numerous takedown attempts, Conti gang became the only recipient of newer TrickBot developments by 2021. By the end of 2021, Conti apparently managed to attract core TrickBot developers and managers, leading to a complete takeover soon thereafter. Although TrickBot has been mostly neutralised, the same group continues to develop new malware, such as BazarBackdoor to gain initial access (Ilascu 2022b).

10 There was also a coordinated cyberattack on digital infrastructures in Montenegro, a NATO-member since 2017, which was partly attributed to the Russia-based Cuba ransomware group, although experts differ on their relationship with the Russian government (Stojanovic 2022).

11 On May 7, 2021, Colonial Pipeline, one of the largest pipeline system for refined oil products in the United States, suffered a ransomware cyberattack that impacted its billing system. As a precautionary measure, the company decided to halt all operations. The resulting fuel shortages disrupted air traffic and led to panic buying at filling station. On May 9, 2021 US President Biden declared a state of emergency (Kerner 2022). This was followed by intense policy debates about the vulnerabilities of critical infrastructures, a lack of mandatory security and reporting standards, and the need to increase pressure on the Russian government to end its practice of providing safe harbours to cybercriminals.

12 This includes anecdotal observations of an intensified cooperation between Russian and Chinese cybercriminals (Schwartz and Yusupov 2022).

13 It should however be noted that Ukrainian cybersecurity officials have recently begun to gather digital evidence for Russian cyberattacks that do constitute war crimes in their opinion (Van Sant 2023).

14 This does not mean that there are no limits to such operations. See the discussion around an alleged DDoS-attack against the leak sites of LockBit in August 2022, possibly conducted by a cybersecurity company on behalf of their client, which was characterised as a dangerous paradigm shift by security experts (Abrams 2022b).

15 The take-down was at least in part motivated by the fear that TrickBot could be used to interfere with the 2020 US Presidential election, thus further corroborating blurring lines between cybercrime and politically motivated cyber operations. See https://www.atlanticcouncil.org/content-series/the-5x5/the-5x5-russias-cyber-statecraft/ (accessed 16 June 2022).

16 Such permissive effects are not necessarily limited to domestic repression alone, considering for example recent reports on the surveillance and intimidation of overseas dissidents by the Chinese government (Farivar 2022). Therefore, even proponents of universal jurisdiction in cases of certain cybercrimes, such as ransomware, emphasise the need to prevent misuse particularly by authoritarian countries (Lubin 2022: 34).

17 At least under some circumstances, as for example within China, authoritarian ruling practices themselves can aggravate the risks of cybercrime. For example, lack of political participation opportunities and nationalist education policies can become drivers of hacktivism, essentially channelling frustration and anger against foreign targets (Webber and Yip 2018). Arguably, there is thus a potential vicious circle between the misuse of cybercrime legislation for political purposes and cybercrime as diversionary action in authoritarian countries.

18 It encompasses the harmonisation of cybercrime laws (Articles 2-12), procedures to investigate and secure electronic evidence (Articles 14-21) and measures of international law enforcement cooperation on cybercrime and any other crime where evidence is on a computer (Articles 23–35) (Council of Europe 2001). While the original Convention lists five "criminal offenses against the confidentiality, integrity and authenticity of computer data and systems" as well as another four "computer-related offenses" (forgery, fraud, child pornography, copyright infringements) – the first additional protocol of 2003 adds acts of a racist and xenophobic nature committed through computers as further cybercrimes (Council of Europe 2003). Currently (January 2023), there are 68 state parties to the Convention and a further 15 have signed it or have been invited to accede.

19 Another legally binding treaty, the UN Convention against Transnational Organized Crime could in some cases also be used as a basis for multilateral cooperation against cybercrime (see World Economic Forum 2020: 9).

20 On 30th November 2022, the EU Commission, the Council of the European Union and the European Parliament agreed on a compromise that includes additional safeguards and remedies to guarantee the protection of fundamental rights (The European Sting 2022).

21 Domestic policy actions will be needed to affect the supply side as well. Within Europe for example, several member state agencies are accused of using Israeli Pegasus software for potentially illegal surveillance practices, leading to calls for Europol to open investigations into governmental misuse (Kabelka 2022b).

22 Whether or not these procedures are effective is an open question though, also bearing in mind that US cybersecurity capacity-building extents to states such as Bahrain, Morocco and the United Arab Emirates, all of which are accused of using spyware and other tools to enable domestic repression (Starks and Nakashima 2023).

23 Due to substantial gaps in incident reporting it bears mentioning that such publicly available figures most likely only constitute the proverbial "tip of the iceberg" (ENISA 2022: 20).

24 Others have speculated about an evolutionary or revolutionary transformation of ransomware as a criminal business model in response to various future scenarios, including more successful law enforcement (Hacquebord et al. 2022; Starks 2002).

References

Abrams, Lawrence (2022a). Hackers use Conti's leaked ransomware to attack Russian companies. BleepingComputer. https://www.bleepingcomputer.com/news/security/hackers-use-contis-leaked-ransomware-to-attack-russian-companies/ (accessed 16 June 2022).

Abrams, Lawrence (2022b). LockBit Ransomware Blames Entrust for DDoS attacks on Leak Sites. BleepingComputer. https://www.bleepingcomputer.com/news/security/lockbit-ransomware-blames-entrust-for-ddos-attacks-on-leak-sites/ (accessed 17 January 2023).

Accenture (2022). Global Incident Report: Threat Actors Divide Along Ideological Lines over the Russia-Ukraine Conflict on Underground Forums. https://acn-marketing-blog.accenture.com/wp-content/uploads/2022/03/UPDATED-ACTI-Global-Incident-Report-Ideological-Divide-Blog-14MARCH22.pdf (accessed 16 June 2022).

Adams, Perri, Dave Aitel, George Perkovich & J.D. Work (2021). Responsible Cyber Offense. 2 August 2021. https://www.lawfareblog.com/responsible-cyber-offense (accessed 12 August 2022).

Allen, Nathaniel (2021). Africa's Evolving Cyber Threats. Africa Center for Strategic Studies, 19 January 2021. https://africacenter.org/spotlight/africa-evolving-cyber-threats/ (accessed 10 August 2022).

Antoniuk, Daryana (2023). How the war in Ukraine has strengthened the Kremlin's ties with cybercriminals. 31st January 2023. https://therecord.media/how-the-war-in-ukraine-has-strengthened-the-kremlins-ties-with-cybercriminals/ (accessed 2 February 2023).

Asociación por los Derechos Civiles (2021). 6th Round of Consultations on the 2nd Additional Protocol to the Budapest Convention on Cybercrime. 30 April 2021. https://rm.coe.int/0900001680a25784 (accessed 13 August 2022).

Australia, Brazil, Canada, Germany, Israel, the Republic of Korea, Mexico, the Netherlands & Singapore (2022). Joint Working Paper on the Establishment of a UN Cyber Points of Contact Network. https://documents.unoda.org/wp-content/uploads/2022/07/Joint-Working-Paper-PoC-Network.pdf (accessed 11 January 2023).

Baer, Merritt (2017). Cybersecurity is a Social Justice Issue. Fels Institute of Government – University of Pennsylvania, 3 November 2017. https://www.fels.upenn.edu/recap/posts/1404 (accessed 9 August 2022).

Barnes, Nicholas (2017). Criminal Politics: An Integrated Approach to the Study of Organized Crime, Politics, and Violence. Perspectives on Politics 15 (4): 967–987.

Bateman, John (2022). Russia's Wartime Cyber Operations in Ukraine: Military Impacts, Influences, and Implications. Carnegie Endowment for International Peace. https://carnegieendowment.org/files/Bateman_Cyber-FINAL21.pdf (accessed 19 January 2023).

BBC (2017). Cyber-attack was about data and not money, say experts. 29 June 2017. https://www.bbc.com/news/technology-40442578 (accessed 4 August 2022).

Bellanova, Rocco & Marieke de Goede (2021). Co-Producing Security: Platform Content Moderation and European Security Integration. Journal of Common Market Studies 60 (5): 1316–1334.

Bender, Bryan (2022). Russia's Space Chief Says Hacking Satellites 'a Cause for War'. Politico. https://www.politico.com/news/2022/03/02/russia-space-chief-hacking-satellites-war-00013211 (accessed 11 January 2023).

Ben-Hassine, Wafa & Dima Samaro (2019). Restricting Cybersecurity, Violating Human Rights: Cybercrime Laws in MENA Region. OpenGlobalRights, 10 January 2019. https://www.openglobalrights.org/restricting-cybersecurity-violating-human-rights/ (accessed 9 August 2022).

Bing, Christopher (2022). Russia-based ransomware group Conti issues warning to Kremlin foes. Reuters. https://www.reuters.com/technology/russia-based-ransomware-group-conti-issues-warning-kremlin-foes-2022-02-25/ (accessed 16 June 2022).

Bitcom (2022). 203 Milliarden Euro Schaden pro Jahr durch Angriffe auf deutsche Unternehmen. https://www.bitkom.org/Presse/Presseinformation/Wirtschaftsschutz-2022 (accessed 18 March 2023).

Blachmann, Yana (2021). North Korean Cyberattacks Can Inspire other Rogue Nations. Venafi Blog, 24 June 2021. https://www.venafi.com/blog/north-korean-cyberattacks-can-inspire-other-rogue-nations (accessed 5 August 2022).

Boes, Sanne & Eric Rutger Leukfeldt (2017). Fighting Cybercrime: A Joint Effort. In: Clark, Robert M. & Simon Hakim (eds.): Cyber-Physical Security: Protecting Critical Infrastructure at the State and Local Level. Cham: Springer: 185–203.

Brady, Sheelagh & Caitríona Heinl (2020). Cybercrime: Current Threats and Responses: A Review of the Research Literature. Department of Justice and Equality of the Republic of Ireland. https://www.drugsandalcohol.ie/33221/1/Cybercrime_-_Current_Threats_and_Responses.pdf (accessed 10 March 2023).

Brzoska, Michael (2000). The Concept of Security Sector Reform. Bonn International Center for Conversion, Brief 15. https://www.bicc.de/uploads/tx_bicctools/brief15.pdf (accessed 4 August 2022).

Bureau, Pierre-Marc (2022). Initial Access Broker Repurposing Techniques in Targeted Attacks against Ukraine. Google Threat Analysis Group, 7 September 2022. https://blog.google/threat-analysis-group/initial-access-broker-repurposing-techniques-in-targeted-attacks-against-ukraine/ (accessed 17 January 2023).

Carmi, Omer (2022). How Threat Actors Are a Click Away From Becoming Quasi-APTs, DarkReading, https://www.darkreading.com/attacks-breaches/how-threat-actors-are-one-click-away-from-becoming-quasi-apts (accessed 16 June 2022).

Carrera, Sergio, Marco Stefan & Valsamis Mitsilegas (2020). Cross-border data access in criminal proceedings and the future of digital justice: Navigating the current legal framework and exploring ways forward within the EU and across the Atlantic. Brussels: Centre for European Policy Studies (CEPS). https://www.ceps.eu/wp-content/uploads/2020/10/TFR-Cross-Border-Data-Access.pdf (accessed 13 August 2022).

Charney, Scott, Erin English, Aaron Kleiner, Nemanja Malisevic, Angela McKay, Jan Neutze & Paul Nicholas (2016). From Articulation to implementation: Enabling Progress on Cybersecurity Norms. Microsoft White Paper. https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/REVmc8 (accessed 6 August 2022).

CNBC Africa (2021). Cyberattacks in Africa comparable to other parts of the globe, says Kaspersky. https://www.cnbcafrica.com/2021/cyberattacks-in-africa-comparable-to-other-parts-of-the-globe-says-kaspersky/ (accessed 16 June 2022).

CNN (2021). US military's hacking unit publicly acknowledges taking offensive action to disrupt ransomware operations. https://edition.cnn.com/2021/12/05/politics/us-cyber-command-disrupt-ransomware-operations/index.html (accessed 16 June 2022).

Collier, Ben, R. Clayton, Alice Hutchins & Daniel L. Thomas (2020). Cybercrime is (often) boring: maintaining the infrastructure of cybercrime economies. Computer Science.

Collier, Jamie (2021). To the Frontline and Beyond: How Ransomware's Operational Details Can Inform Policy and Strategy. https://offensivecyber.org/2021/10/22/frontline-and-beyond/ (accessed 16 June 2022).

Corcoran, Brian (2020). A comparative Study of Domestic Laws Constraining Private Sector Active Defense Measures in Cyberspace. Harvard National Security Journal 11 (1): 1–53.

Council of Europe (2021). Summary of comments on opinions by Council of Europe Committees and submissions by other stakeholders on the draft 2nd Additional Protocol to the Convention on Cybercrime (May 2021), 28th May 2021, https://rm.coe.int/0900001680a2aa1d (accessed 13th August 2022).

Council of Europe (2018). Modernised Convention for the Protection of Individuals with Regard to the Processing of Personal Data. https://search.coe.int/cm/Pages/result_details.aspx?ObjectId=09000016807c65bf (accessed 20 March 2023).

Council of Europe (2017). Assessment Report on Mutual Legal Assistance: Follow up given by Parties and Observers, Cybercrime Convention Committee (T-CY). https://rm.coe.int/t-cy-2017-2-mla-follow-up-rep/168076d55f (accessed 11 August 2022).

Council of Europe (2003). Additional Protocol to the Convention on Cybercrime, concerning the criminalisation of acts of a racist and xenophobic nature committed through computer systems. https://rm.coe.int/168008160f (accessed 11 August 2022).

Council of Europe (2001). Convention on Cybercrime. https://rm.coe.int/1680081561 (accessed 11 August 2022).

Cox, Joseph (2017). Revenge Hacking is Hitting the Big Time. The Daily Beast, 19 September 2017. https://www.thedailybeast.com/inside-the-shadowy-world-of-revenge-hackers (accessed 5 August 2022).

CyberPeace Institute (2021). Big Statements Matter Little for Victims. https://cyberpeaceinstitute.org/blog-series-reconceptualizing-ransomware/ (accessed 16 June 2022).

Delcker, Janosch (2022). Ransomware: Cyber Criminals are Coming for the Global South. Deutsche Welle, 28 August 2022. https://www.dw.com/en/ransomware-cyber-criminals-are-coming-for-the-global-south/a-62917234 (accessed 17 January 2023).

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

Doyle, Peyton (2022). How Russian sanctions may be helping US cybersecurity. TechTarget. https://www.techtarget.com/searchsecurity/news/252521530/How-Russian-sanctions-may-be-helping-US-cybersecurity (accessed 16 June 2022).

Droz, Serge & Daniel Stauffacher (2018). Trust and Attribution in Cyberspace: A Proposal for an Independent Network of Organisations Engaging in Attribution Peer-Review. Geneva: ICT4Peace Foundation. https://ict4peace.org/wp-content/uploads/2019/07/ICT4Peace-2019-Trust-and-Attribution-in-Cyberspace.pdf (accessed 6 August 2022).

Electronic Frontier Foundation (2023). EFF and Partners Call Out Threats to Free Expression in Draft Text as UN Cybersecurity Treaty Negotiations Resume. https://www.eff.org/deeplinks/2023/01/eff-and-partners-call-out-threats-free-expression-draft-text-un-cybersecurity (accessed 11 January 2023).

ENISA (2022). ENISA Threat Landscape for Ransomware Attacks. https://www.enisa.europa.eu/publications/enisa-threat-landscape-for-ransomware-attacks (accessed 17 January 2023).

ENISA (2021). Data Pseudonymisation: Advanced Techniques & Use Cases. https://www.enisa.europa.eu/publications/data-pseudonymisation-advanced-techniques-and-use-cases (accessed 12 August 2022).

Eoyang, Mieke, Allison Peters, Ishan Mehta & Brandon Gaskew (2018). To Catch a Hacker: Toward a Comprehensive Strategy to Identify, Pursue, and Punish Malicious Cyber Actors. Third Way, 29 October 2018, https://www.thirdway.org/report/to-catch-a-hacker-toward-a-comprehensive-strategy-to-identify-pursue-and-punish-malicious-cyber-actors (accessed 20 March 2023).

ESET (2022). Threat Report T 1 2022. https://www.welivesecurity.com/wp-content/uploads/2022/06/eset_threat_report_t12022.pdf (accessed 16 June 2022).

Eurojust (2022). Cybercrime Judicial Monitor. Issue 7. https://www.eurojust.europa.eu/sites/default/files/assets/cybercrime-judicial-monitor-issue-7-2022.pdf (accessed 17 January 2023).

Euronews (2022). Russian-speaking ransomware gang threatens to overthrow Costa Rica government after cyberattack. https://www.euronews.com/next/2022/05/17/russian-speaking-ransomware-gang-threatens-to-overthrow-costa-rica-government-after-cyber- (accessed 16 June 2022).

European Commission (2015). Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of The Regions: The European Agenda on Security, COM (2015). Strasbourg: 28th April 2015, 185 final. https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52015DC0185&from=EN (accessed 13 August 2022).

European Union (2016). REGULATION (EU) 2016/679 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation). Official Journal of the European Union, 4th May 2016. https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679&from=EN (accessed 13 August 2022).

Europol (2021). Internet Organised Crime Threat Assessment 2021. https://www.europol.europa.eu/cms/sites/default/files/documents/internet_organised_crime_threat_assessment_iocta_2021.pdf (accessed 17 January 2023).

Farivar, Masood (2022). China Steps Up Intimidation, Harassment of Chinese Dissidents in US. https://www.voanews.com/a/us-officials-warn-of-china-s-transnational-repression-operations/6658166.html (accessed 17 January 2023).

Feaver, Peter & Kenneth Geers (2017). "When the Urgency of Time and Circumstances Clearly Does Not Permit...": Pre-delegation in Nuclear and Cyber Scenarios. Carnegie Endowment of International Peace, 16th October 2017. https://carnegieendowment.org/2017/10/16/when-urgency-of-time-and-circumstances-clearly-does-not-permit-.-.-.-pre-delegation-in-nuclear-and-cyber-scenarios-pub-73417 (accessed 16 August 2022).

Flashpoint (2022). Raid Forums Is Down. Who's Behind Its Apparent Seizure? https://flashpoint.io/blog/raid-forums-seizure/ (accessed 16 June 2022).

Gleditsch, Kristian Skrede & Andrea Ruggeri (2010). Political Opportunity Structures, Democracy and Civil War. Journal of Peace Research 47 (3): 299–310.

Glick, Veronica & David Simon (2022). Cyber Symposium – Private Sector View on the Use of Force. Lieber Institute/West Point. https://lieber.westpoint.edu/private-sector-view-use-force/ (accessed 10 January 2023).

Global Initiative against Transnational Organized Crime (2022). Conviction of Samira Sabou and Moussa Aksar sets dangerous precedent for Niger. https://globalinitiative.net/analysis/statement4122/ (accessed 16 June 2022).

Gomez, Miguel Alberto (2021). Understanding Public Reactions to Cybersecurity Incidents. https://www.realinstitutoelcano.org/en/analyses/understanding-public-reactions-to-cybersecurity-incidents/ (accessed 11 January 2023).

Goodin, Dan (2021). It's ransomware, or maybe a disk wiper, and it's striking targets in Israel. 25 May 2021. https://arstechnica.com/gadgets/2021/05/disk-wiping-malware-with-irananian-fingerprints-is-striking-israeli-targets/ (accessed 4 August 2022).

Goodin, Dan (2017). Tuesday's massive ransomware outbreak was, in fact, something much worse. 28 June 2017. https://arstechnica.com/information-technology/2017/06/petya-outbreak-was-a-chaos-sowing-wiper-not-profit-seeking-ransomware/ (accessed 4 August 2022).

Greenberg, Andy (2022). Hackers Planted Files to Frame an Indian Priest Who Died in Custody. Wired, 13 December 2022. https://www.wired.com/story/modified-elephant-stan-swamy-hacked-evidence-frame-bhima-koregaon-16/ (accessed 19 January 2023).

Greig, Jonathan (2022). Biden warns of US 'cyber' response after Ukraine says computers wiped during attack. ZD Net. https://www.zdnet.com/article/biden-threatens-cyber-response-after-ukraine-says-computers-wiped-during-attack/ (accessed 16 June 2022).

Group of Governmental Experts on Advancing Responsible State Behaviour in Cyberspace in the Context of International Security (2021). Report. https://front.un-arm.org/wp-content/uploads/2021/08/A_76_135-2104030E-1.pdf (accessed 29 June 2022).

Grünewald, Zoë (2022). How the War in Ukraine is Reshaping the Dark Web. The New Statesman. https://www.newstatesman.com/spotlight/cybersecurity/2022/08/ukraine-war-cyber-attacks-the-dark-web (accessed 17 January 2023).

Gulf Centre for Human Rights (2018). Mapping Cybercrime Laws and Violations of Digital Rights in the Gulf and Neighbouring Countries. https://www.gc4hr.org/report/view/78 (accessed 13 August 2022).

Hacquebord, Feike, Stephen Hilt & David Sancho (2022). The Near and Far Future of Ransomware Business Models. TrendMicro. https://documents.trendmicro.com/assets/white_papers/wp-the-near-and-far-future-of-ransomware.pdf (accessed 19 January 2023).

Hakmeh, Joyce & Tatiana Tropina (2021). Russia's Vision for a Cybercrime Treaty. Directions. https://directionsblog.eu/russias-vision-for-a-cybercrime-treaty/ (accessed 16 June 2022).

Hakmeh, Joyce & Kerstin Vignard (2021). ICTs, International Security, and Cybercrime. Geneva: UNIDIR.

Hakmeh, Joyce & Allison Peters (2020). A New UN Cyber Treaty? The Way Forward for Supporters of an Open, Free and Secure Internet. Council on Foreign Relations, 13 January 2020. https://www.cfr.org/blog/new-un-cybercrime-treaty-way-forward-supporters-open-free-and-secure-internet (accessed 5 August 2022).

Handler, Simon (2021). The Strategic Intelligence Value of Ransomware. Lawfare. https://www.lawfareblog.com/strategic-intelligence-value-ransomware (accessed 16 June 2022).

Hansel, Mischa (2018). Cyber-Attacks and Psychological IR Perspectives: Explaining Misperceptions and Escalation Risks. Journal of International Relations and Development 21 (3): 523–551.

Hardcastle, Jessica L. (2022). Crooks use fake emergency data requests to get personal info out of Big Tech – report. The Register. https://www.theregister.com/2022/04/02/in_brief_security/ (accessed 16 June 2022).

Healey, Jason (2022). Soldiers, Statesmen and Cyber Crises: Cyberspace and Civil-Military Relations, Lawfare Blog, 16 March 2022. https://www.lawfareblog.com/soldiers-statesmen-and-cyber-crises-cyberspace-and-civil-military-relations (accessed 20 March 2023).

Healey, Jason (2021). When Should U.S. Cyber Command Take Down Criminal Botnets? Lawfare Blog, 26 April 2021. https://www.lawfareblog.com/when-should-us-cyber-command-take-down-criminal-botnets (accessed 4 August 2022).

Healy, Jason, John C. Mallery, Klara Thotova Jordan & Nathaniel V. Youd (2014). Confidence-Building Measures in Cyberspace: A Multistakeholder-Approach for Stability and Security. Atlantic Council https://www.atlanticcouncil.org/wp-content/uploads/2014/11/Confidence-Building_Measures_in_Cyberspace.pdf (accessed 6 August 2022).

Heidtmann, Jan (2021). Wie Hacker einen Landkreis erpressen. Süddeutsche Zeitung, 15 July 2021. https://www.sueddeutsche.de/politik/hacker-anhalt-bitterfeld-1.5353265 (accessed 4 August 2022).

Hoffmann, Wyatt & Steven Nyikos (2018). Governing Private Sector Self-Help in Cyberspace: Analogies from the Physical World. Carnegie Endowment for International Peace. https://carnegieendowment.org/files/Hoffman_Nyikos_Self_Help_FINAL_WEB_bio_edit.pdf (accessed 5 August 2022).

Holdemann, Eric (2022). More Developments on Cybercrime and Russia. https://www.govtech.com/em/emergency-blogs/disaster-zone/more-developments-on-cyber-crime-and-russia (accessed 17 January 2023).

Housen-Couriel (2020). Hacking Back under International Law: Toward Effective Remedies against Cyberattacks for Non-State Actors. In: Gabi Siboni & Limor Ezioni (eds.): Cybersecurity and Legal-Regulatory Aspects. New Jersey et al.: World Scientific: 103–133.

Ifeanyi-Ajufo, Nnenna (2022). International Cooperation and Cybersecurity in Africa. EU Cyber Directions Blog. https://directionsblog.eu/international-cooperation-and-cybersecurity-in-africa/ (accessed 19 January 2023).

Ilascu, Ionut (2022a). Ransomware gangs, hackers pick sides over Russia invading Ukraine. https://www.bleepingcomputer.com/news/security/ransomware-gangs-hackers-pick-sides-over-russia-invading-ukraine/ (accessed 16 June 2022).

Ilascu, Ionut (2022b). Conti ransomware gang takes over TrickBot malware operation https://www.bleepingcomputer.com/news/security/conti-ransomware-gang-takes-over-trickbot-malware-operation/ (accessed 22 March 2023).

Ilievski, Aleksandar & Igor Bernik (2016). Social-Economic Aspects of Cybercrime. Innovative Issues and Approaches in Social Sciences 9 (3): 8–22.

Internet Society (2018). The Internet and Extra-Territorial Effects of Laws. Internet Society Concept Note. https://www.internetsociety.org/wp-content/uploads/2018/10/The-Internet-and-extra-territorial-application-of-laws-EN.pdf (accessed 5 August 2022).

Interpol (2022). 2022 Interpol Global Crime Trend Summary Report. https://www.interpol.int/How-we-work/Criminal-intelligence-analysis2/Our-analysis-reports (accessed 18 January 2023).

Interpol (2021). Online African Organized Crime from Surface to Darkweb. https://south.euneighbours.eu/wp-content/uploads/2022/07/INTERPOL-report-1.pdf (accessed 20 March 2023).

Jenkins, Luke, Emiel Haeghebaert, Alice Revelli & Ben Read (2022). Likely Iranian Threat Actor Conducts Politically Motivated Disruptive Activity Against Albanian Government Organizations. Mandiant, 4th August 2022. https://www.mandiant.com/resources/blog/likely-iranian-threat-actor-conducts-politically-motivated-disruptive-activity-against (accessed 17 January 2023).

Jensen, Benjamin & Brandon Valeriano (2019). What Do We Know about Cyber Escalation? Observations from Simulations and Surveys, Atlantic Council Issue Brief, https://www.atlanticcouncil.org/wp-content/uploads/2019/11/What_do_we_know_about_cyber_escalation_.pdf (accessed 27 March 2023).

Jensen, Benjamin & J.D. Work (2018). Cyber Civil-Military Relations: Balancing Interests on the Digital Frontier, War on the Rocks Blog, 4 September 2018, https://warontherocks.com/2018/09/cyber-civil-military-relations-balancing-interests-on-the-digital-frontier/ (accessed 20 March 2023).

Jo, Hyeran & Beth A. Simmons (2016). Can the International Criminal Court Deter Atrocity? International Organization 70 (3): 443–475.

Jun, Jenny (2021). The Political Economy of Ransomware. War on the Rocks, 2 June 2021. https://warontherocks.com/2021/06/the-political-economy-of-ransomware/ (accessed 10 August 2022).

Kabelka, Laura (2022a). EU Cybersecurity Agency Chief Warns of Cyberthreats and Spillovers. https://www.euractiv.com/section/cybersecurity/news/eu-cybersecurity-agency-chief-warns-of-cyberthreats-and-spillovers/ (accessed 19 January 2023).

Kabelka, Laura (2022b). EU's Competences to Handle Spyware Abuse in Question. 30 August 2022. https://www.euractiv.com/section/digital/news/eus-competences-to-handle-spyware-abuse-in-question/ (accessed 17 January 2023).

Kapko, Matt (2022). Ransomware Attacks Shift beyond US Borders. https://www.cybersecuritydive.com/news/ransomware-shift-global/638089/ (accessed 18 January 2023).

Kaspersky (2023). Come to the Dark Side: Hunting IT Professionals on the Dark Web. 30 January 2023 https://securelist.com/darknet-it-headhunting/108526/ (accessed 1 February 2023).

Katagiri, Nori (2021). Why international law and norms do little in preventing non-state cyber attacks. Journal of Cybersecurity 7 (1): 1–9.

Kerner, Sean Michael (2022). Colonial Pipeline hack explained: Everything you need to know. https://www.techtarget.com/whatis/feature/Colonial-Pipeline-hack-explained-Everything-you-need-to-know (accessed 17 March 2023).

Kirchgaessner, Stephanie, Paul Lewis, David Pegg, Sam Cutler, Nina Lakhani & Michael Safi (2021). Revealed: Leak Uncovers Global Abuse of Cyber-Surveillance Weapon. The Guardian, 18 July 2021. https://www.theguardian.com/world/2021/jul/18/revealed-leak-uncovers-global-abuse-of-cyber-surveillance-weapon-nso-group-pegasus (accessed 16 August 2022).

Knodel, Mallory (2002). The Three Top Issues to Address for the Global Cybercrime Treaty. Center for Democracy & Technology, 28 October 2022. https://cdt.org/insights/the-three-top-issues-to-address-for-the-global-cybercrime-treaty/ (accessed 18 January 2023).

Kolochenko, Ilia (2016). Cybercrime: The Price of Inequality. Forbes, 19 December 2016. https://www.forbes.com/sites/forbestechcouncil/2016/12/19/cybercrime-the-price-of-inequality/?sh=5f16901d7d01 (accessed 9 August 2022).

Kommersant (2021). Draft United Nations Convention on Countering the Use of Information and Communication Technologies for Criminal Purposes. Unofficial Translation. https://www.kommersant.ru/docs/2021/RF_28_July_2021_-_E.pdf (accessed 12 August 2022).

Koops, Bert-Jaap & Morag Goodwin (2014). Cyberspace, the Cloud, and Cross-Border Criminal Investigation: The Limits and Possibilities of International Law. Tilburg Law School Research Paper. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2698263 / (accessed 23 September 2022).

Korzak, Elaine (2021). Russia's Cyber Policy Efforts in the United Nations. https://ccdcoe.org/uploads/2021/06/Elaine_Korzak_Russia_UN.docx.pdf (accessed 27 June 2022).

Kraft, Wolfgang W. & Claudia Streit (2011). Ideas on the Establishment of an International Court for Cyber Crime. World Council for Law Firms and Justice: White Paper. http://www.wclf.de/cybercrime_court_en.html?file=tl_files/Media/Download/FINAL-CYBER-COURT-ENGLISH.pdf (accessed 6 August 2022).

Krebs, Brian (2021). Ransomware Gangs and the Name Game Distraction. Krebs on Security, 5 August 2021. https://krebsonsecurity.com/2021/08/ransomware-gangs-and-the-name-game-distraction/ (accessed 9 August 2022).

Kshetri, Nir (2019). Cybercrime and Cybersecurity in Africa. Journal of Global Information Technology Management 22 (2): 77–81.

Kshetri, Nir (2010). Diffusion and Effects of Cyber-Crime in Developing Economies. Third World Quarterly 31 (7): 1057–1079.

Lachow, Irv & Taylor Grossman (2018). Cyberwar Inc: Examining the Role of Companies in Offensive Cyber Operations. In: Herbert Lin & Amy Zegart (eds.): Bytes, Bombs and Spies: The Strategic Dimensions of Offensive Cyber Operations. Washington DC, 379–399.

Ladegard, Isak (2019). "I Pray That We Will Find a Way to Carry on This Dream": How a Law Enforcement Crackdown United an Online Community. Critical Sociology 45 (4–5): 631–646.

Locke, Rachel (2012). Organized Crime, Conflict, and Fragility: A New Approach. International Peace Institute. https://www.files.ethz.ch/isn/146111/2012-07.pdf (accessed 23 September 2022).

Lubin, Asaf (2022). The Law and Politics of Ransomware. Vanderbilt Journal of Transnational Law 55, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4181964 (accessed 17 January 2023).

Maschmeyer, Lennart & Nadiya Kostyuk (2022). There is No Cyber 'Shock and Awe': Plausible Threats in the Ukrainian Conflict. War on the Rocks. https://warontherocks.com/2022/02/there-is-no-cyber-shock-and-awe-plausible-threats-in-the-ukrainian-conflict/ (accessed 16 June 2022).

Manky, Derek (2021). Ransomware Takedowns Underscore Need for Private-Public Cybersecurity Collaboration. Security Week, 5 March 2021. https://www.securityweek.com/ransomware-takedowns-underscore-need-private-public-cybersecurity-collaboration (accessed 12 August 2022).

Mansfield, Edward D.S. & Jack Snyder (2005). Why Emerging Democracies Go to War. Cambridge, MA: MIT Press.

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

Mchangama, Jacob & Joelle Fiss (2019). Germany's Online Crackdowns Inspire the World's Dictators. Foreign Policy, https://foreignpolicy.com/2019/11/06/germany-online-crackdowns-inspired-the-worlds-dictators-russia-venezuela-india/ (accessed 17 March 2023).

Microsoft (2023). Fog of War: How the Ukraine Conflict Transformed the Cyber Threat Landscape. https://services.google.com/fh/files/blogs/google_fog_of_war_research_report.pdf (accessed 16 March 2023).

Microsoft (2022). New "Prestige" Ransomware Impacts Organizations in Ukraine and Poland. 14 October 2022. https://www.microsoft.com/en-us/security/blog/2022/10/14/new-prestige-ransomware-impacts-organizations-in-ukraine-and-poland/ (accessed 18 January 2023).

Microsoft (2021). Evolving trends in Iranian threat actor activity. MSTIC presentation at CyberWarCon 2021. https://www.microsoft.com/security/blog/2021/11/16/evolving-trends-in-iranian-threat-actor-activity-mstic-presentation-at-cyberwarcon-2021/ (accessed 16 June 2022).

Mikanagi, Tomohiro (2021). Application of the Due Diligence Principle to Cyber Operations. International Law Studies 97: 1019–1038.

Morgan, Steve (2020). Cybercrime To Cost The World $10.5 Trillion Annually By 2025. 13 November 2020. https://cybersecurityventures.com/cybercrime-damages-6-trillion-by-2021/ (accessed 20 March 2023).

Nichols, Michelle (2023). Exclusive: Record-Breaking 2022 for North Korea Crypto Theft, UN Report Says. Reuters. https://www.reuters.com/technology/record-breaking-2022-north-korea-crypto-theft-un-report-2023-02-06/ (accessed 16 March 2023).

Nichols, Michelle (2019). North Korea took $2 billion in cyberattacks to fund weapons program: U.N. report. Reuters. https://www.reuters.com/article/us-northkorea-cyber-un-idUSKCN1UV1ZX (accessed 16 June 2022).

Nichols, Shaun (2022). Russian Cyber Attacks on Ukraine driven by Government groups. https://www.techtarget.com/searchsecurity/news/252523950/Russian-cyber-attacks-on-Ukraine-driven-by-government-groups (accessed 17 January 2023).

Nolte, Amina & Carola Westermeier (2020). Between Public and Private: The Co-production of Infrastructural Security. Politikon – South African Journal of Political Studies 47 (1): 62–80.

Nyabola, Nanjala (2018). Digital Democracy, Analogue Politics: How the Internet Era is Transforming Politics in Kenya. London: ZedBooks.

Office of the Privacy Commissioner of Canada (2021). Re: Preparing a 2nd Additional Protocol to the Budapest Convention on Cybercrime. Letter. https://rm.coe.int/0900001680a25785 (accessed 13 August 2022).

O'Neill, Patrick Howell (2021a). Chinese Hackers Disguised themselves as Iran to Target Israel. MIT Technology Review, 10 August 2021. https://www.technologyreview.com/2021/08/10/1031622/chinese-hackers-false-flag-iran-israel-fireeye/ (accessed 12 August 2022).

O'Neill, Patrick Howell (2021b). French spyware bosses indicted for their role in the torture of dissidents. MIT Technology Review, 22 June 2021. https://www.technologyreview.com/2021/06/22/1026777/france-spyware-amesys-nexa-crimes-against-humanity-libya-egypt/ (accessed 5 August 2022).

Paganini, Pierluigi (2022). RansomBoggs Ransomware Hit several Ukrainian Entities: Experts Attribute it to Russia. 28 November 2022 https://securityaffairs.co/139028/cyber-warfare-2/ransomboggs-ransomware-targeted-ukraine.html (accessed 18 January 2023).

Pavlova, Pavlina & Charlotte Lindsey (2023). A Year of United Nations Cybercrime Negoations. CyberPeace Institute, 28 February 2023. https://cyberpeaceinstitute.org/news/a-year-of-united-nations-cybercrime-negotiations-the-message-of-the-multi-stakeholder-manifesto-remains-central-as-the-process-moves-forward/ (accessed 16 March 2023).

Pascucci, Peter & Kurt Sanger (2021). Revisiting a Framework on Military Takedowns against Cybercriminals. Lawfare, 2 July 2021. https://www.lawfareblog.com/revisiting-framework-military-takedowns-against-cybercriminals (accessed 5 August 2022).

Patrick, Colin (2019). Debugging the Tallinn Manual 2.0's Application of the Due Diligence Principle to Cyber Operations. Washington International Law Journal 8 (2): 521–604.

Pearson, James & Raphael Satter (2022). Analysis: Russian ransomware attacks on Ukraine muted by leaks, insurance woes. https://www.reuters.com/technology/russian-ransomware-attacks-ukraine-muted-by-leaks-insurance-woes-2022-03-01/ (accessed 11 January 2023).

Perlroth, Nicole & Adam Satariano (2021). Irish Hospitals Are Latest to Be Hit by Ransomware Attack. The New York Times, 20 May 2021. https://www.nytimes.com/2021/05/20/technology/ransomware-attack-ireland-hospitals.html (accessed 4 August 2022).

Peters, Allision & Michael Garcia (2020). A Roadmap to Strengthen US Cyber Enforcement. Third Way, 9 November 2020. https://thirdway.imgix.net/pdfs/override/A-Roadmap-to-Strengthen-US-Cyber-Enforcement.pdf (accessed 10 August 2022).

Reuters (2022). Albania Cuts Iran Ties over Cyberattack: U.S. Vows further Action. https://www.reuters.com/world/albania-cuts-iran-ties-orders-diplomats-go-after-cyber-attack-pm-says-2022-09-07/ (accessed 10 January 2023).

Rio, Victoire (2020). The Role of Social Media in Fomenting Violence: Myanmar. Toda Peace Institute: Policy Brief No. 78. https://toda.org/assets/files/resources/policy-briefs/t-pb-78_victoire-rio_role-of-social-media-in-fomenting-violence-myanmar.pdf (accessed 10 August 2022).

Robertson, Jordan & Michael Riley (2014). Corporations Warned not to Hack Back. Insurance Journal, 31 December 2014. https://www.insurancejournal.com/news/national/2014/12/31/351326.htm (accessed 5 August 2022).

Rodriguez, Katitza & Meri Baghdasaryan (2022). UN Committee To Begin Negotiating New Cybercrime Treaty Amid Disagreement Among States Over Its Scope. Electronic Frontier Foundation. https://www.eff.org/de/deeplinks/2022/02/un-committee-begin-negotiating-new-cybercrime-treaty-amid-disagreement-among (accessed 16 June 2022).

Rodriguez, Katitza (2017). The Cybercrime Convention's New Protocol Needs to Uphold Human Rights. Electronic Frontier Foundation, 18 September 2017. https://www.eff.org/deeplinks/2017/09/cybercrime-conventions-new-protocol-needs-uphold-human-rights (accessed 13 August 2022).

Ropek, Lucas (2021). The Ex-NSA Operative Cyber-Mercenary Scandal Shows the Spyware Industry Is Totally Out of Control. Gizmodo, 16 September 2021. https://gizmodo.com/the-ex-nsa-operative-cyber-mercenary-scandal-shows-the-1847688488 (accessed 23 September 2022).

Ross, Michael L. (2015). What Have We Learned about the Resource Curse? Annual Review of Political Science 18: 239–259.

Rudesill, Dakota S. (2020). Cyber Operations, Legal Secrecy, and Civil-Military Relations. In: Lionel Beehner, Risa Brooks & Daniel Maurer (eds.): Reconsidering American Civil-Military Relations: The Military, Society, Politics, and Modern War. Oxford: Oxford University Press: 245–262.

Sadowski, James & Casey Charrier (2023). Move, Patch, Get Out the Way: 2022 Zero-Day Exploitation Continues at an Elevated Pace. Mandiant, 20th March 2023. https://www.mandiant.com/resources/blog/zero-days-exploited-2022 (accessed 21 March 2023).

Schallbruch, Martin, Michael Huth, Leif-Nissen Lundbæk, Clara Herdeanu & Lola Attenberger (2021). Künstliche Intelligenz für den öffentlichen Sektor: Masked Federated Learning als datenschutzfreundliche Lösung. Berlin: Digital Society Institute/European School of Management & Technology/Xayn: Positionspaper. https://faculty-research.esmt.berlin/sites/faculty/files/2021-06/Xayn_DSI_Positionpaper_DE.pdf (accessed 12 August 2022).

Schjolberg, Stein (2012). An International Criminal Tribunal for Cyberspace (ICTC): Recommendations for potential new global legal mechanisms against global cyberattacks and other global cybercrimes. EastWest Institute (EWI) Cybercrime Legal Working Group. https://www.cybercrimelaw.net/documents/ICTC.pdf (accessed 6 August 2022).

Schmidle, Nicholas (2018). The Digital Vigilantes Who Hack Back. The New Yorker, 30 April 2018. https://www.newyorker.com/magazine/2018/05/07/the-digital-vigilantes-who-hack-back (accessed 16 June 2022).

Schmitt, Michael (2015). In Defense of Due Diligence in Cyberspace. The Yale Law Journal Forum 125: 68–81.

Schwartz, Delilah & Naomi Yusupov (2022). Could Russian and Chinese Cybercriminals Team Up Against the West? The National Interest, 2 August 2022. https://nationalinterest.org/blog/techland-when-great-power-competition-meets-digital-world/could-russian-and-chinese (accessed 17 January 2023).

Schwartz, Matthew J. (2022). Cause for Concern? Ransomware Strains Trace to North Korea. BankInfoSecurity. https://www.bankinfosecurity.com/blogs/cause-for-concern-ransomware-strains-trace-to-north-korea-p-3232 (accessed 16 June 2022).

Scroxton, Alex (2022). Cyber Criminal Forum Targets only Russia. 12 August 2022. https://www.computerweekly.com/news/252523772/Cyber-criminal-forum-targets-only-Russia (accessed 17 January 2023).

Shany, Yuval & Michael Schmitt (2020). An International Attribution Mechanism for Hostile Cyber Operations. International Law Studies 96: 196–222.

Smith, Maggie, Erica D. Lonergan & Nick Starck (2022). What Impact, if Any, Does Killnet Have? Lawfare, 21 October 2022. https://www.lawfareblog.com/what-impact-if-any-does-killnet-have (accessed 18 January 2023).

Smith, Zhanna Malekos & Eugenia Lostri & James A. Lewis (2020). The Hidden Costs of Cybercrime, McAfee Report, https://companies.mybroadband.co.za/axiz/files/2021/02/eBook-Axiz-McAfee-hidden-costs-of-cybercrime.pdf (accessed 20 March 2023).

Soesanto, Stefan (2021). Hacking Back Unpacked: an Eye for an Eye? Not so fast. CSS Blog. https://isnblog.ethz.ch/security/hacking-back-unpacked-an-eye-for-an-eye-not-so-fast (accessed 5 August 2022).

Starks, Tim & Ellen Nakashima (2023). The Abraham Accords Expand with Cybersecurity Collaboration. 31 January 2023. https://www.washingtonpost.com/politics/2023/01/31/abraham-accords-expand-with-cybersecurity-collaboration/ (accessed 1 February 2023).

Starks, Tim (2022). Is the Drop in Ransomware Numbers and Illusion? The Washington Post, 17 August 2022. https://www.washingtonpost.com/politics/2022/08/17/is-drop-ransomware-numbers-an-illusion/ (accessed 19 January 2023).

Stojanovic, Dusan (2022). Montenegro Wrestles with Massive Cyberattack: Russia Blamed. https://apnews.com/article/russia-ukraine-nato-technology-hacking-religion-5c2bd851027b56a77eaf9385b7d5d741 (accessed 17 January 2023).

Swali, Amrit & Esther Naylor (2021). Closing the space between cybercrime and cybersecurity. Chatham House, 29 May 2021. https://www.chathamhouse.org/2021/05/closing-space-between-cybercrime-and-cybersecurity (accessed 6 August 2022).

Swiatkowska, Joanna (2020). Tackling cybercrime to unleash developing countries' digital potential. Pathways for Prosperity Commission: Background Paper. https://pathwayscommission.bsg.ox.ac.uk/sites/default/files/2020-01/tackling_cybercrime_to_unleash_developing_countries_digital_potential.pdf (accessed 6 August 2022).

Tait, Matt (2021). The Kaseya Ransomware Attack Is a really Big Deal. Lawfare, 5 July 2021. https://www.lawfareblog.com/kaseya-ransomware-attack-really-big-deal (accessed 9 August 2022).

The Cyber Peace Institute (2021). Playing with Lives: Cyberattacks on Healthcare are Attacks on People. https://cyberpeaceinstitute.org/report/2021-03-CyberPeaceInstitute-SAR001-Healthcare.pdf (accessed 4 August 2022).

The Cyber Wire (2023). Ukraine at D+347: Hacktivism, Privateering, and Diversionary Ops. https://thecyberwire.com/stories/862634b2d3ba4ae6bb766779e385e159/ukraine-at-d347-hacktivism-privateering-and-diversionary-ops (accessed: 2 March 2023).

The European Sting (2022). e-Evidence: Commission Welcomes Political Agreement to Strengthen Cross-border Access for Criminal Investigations. 30 November 2022. https://europeansting.com/2022/11/30/e-evidence-commission-welcomes-political-agreement-to-strengthen-cross-border-access-for-criminal-investigations/ (accessed 19 January 2023).

The White House (2021). Remarks by President Biden at the Office of the Director of National Intelligence. 27 July 2021, https://www.whitehouse.gov/briefing-room/speeches-remarks/2021/07/27/remarks-by-president-biden-at-the-office-of-the-director-of-national-intelligence/ (accessed 27 March 2023).

Thomas, Troy S., Stephen D. Kiser & William D. Casebeer (2005). Warlords Rising: Confronting Violent Non-State Actors. London et al.: Lexington Books.

Townsend, Kevin (2021). Experts Analyze Proposed Bill Allowing Private Entities to 'Hack Back'. Security Week. https://www.securityweek.com/experts-analyze-proposed-bill-allowing-private-entities-hack-back%E2%80%99 (accessed 16 June 2022).

Toulas, Bill (2022). Chinese hackers use ransomware as decoy for cyber espionage. BleepingComputer. https://www.bleepingcomputer.com/news/security/chinese-hackers-use-ransomware-as-decoy-for-cyber-espionage/ (accessed 17 January 2023).

Trellix (2022). In the Crosshairs: Organizations and Nation-State Cyber Attacks. https://www.trellix.com/en-us/assets/docs/trellix-csis-organizations-and-nation-state-cyber-threats-report.pdf (accessed 17 January 2023).

United Nations (2022). Consolidated negotiating document on the general provisions and the provisions on criminalization and on procedural measures and law enforcement of a comprehensive international convention on countering the use of information and communications technologies for criminal purposes. A/AC.291/16. https://www.unodc.org/documents/Cybercrime/AdHocCommittee/4th_Session/Documents/A_AC291_16_Advance_Copy.pdf (accessed 19 January 2023).

United Nations General Assembly (2021). Open-Ended Working Group on Development in the Field of Information and Telecommunications in the Context of International Security. Final Report. https://front.un-arm.org/wp-content/uploads/2021/03/Final-report-A-AC.290-2021-CRP.2.pdf (accessed 26 June 2022).

United Nations Office on Drugs and Crime (n.d.). Cybercrime. https://www.unodc.org/unodc/encybercrime/global-programme-cybercrime.html (accessed 13 August 2022).

United States National Security Agency & United States Federal Bureau of Investigation & United States Cybersecurity and Infrastructure Security Agency & United States Department of Health and Human Services (HHS), the Republic of Korea (ROK) National Intelligence Service (NIS) & the ROK Defense Security Agency (DSA) (2023). #StopRansomware: Ransomware Attacks on Critical Infrastructure Fund DPRK Malicious Cyber Activities, Cybersecurity Advisory (CSA). https://media.defense.gov/2023/Feb/09/2003159161/-1/-1/0/CSA_RANSOMWARE_ATTACKS_ON_CI_FUND_DPRK_ACTIVITIES.PDF (accessed: 16 March 2023).

Uren, Tom (2022). Pulling Russia's Plug a Gift to Putin: Seriously Risky Business. https://srslyriskybiz.substack.com/p/srsly-risky-biz-thursday-march-17?s=r (accessed 16 June 2022).

Valeriano, Brandon & Ryan C. Maness (2014). The Dynamics of Cyber Conflict between Rival Antagonists, 2001–11. Journal of Peace Research 51 (3): 347–360.

Van de Velde (2022). Opinion: The Intellectual Mistakes that Crippled U.S. Cyber Policy. Cyberscoop, 3 August 2022. https://www.cyberscoop.com/intellectual-mistakes-crippled-cyber-policy/ (accessed 17 January 2023).

Van Sant, Shannon (2023). Kyiv argues Russian cyberattacks could be war crimes. https://www.politico.eu/article/victor-zhora-ukraine-russia-cyberattack-infrastructure-war-crime/ (accessed 11 January 2023).

Vicens, AJ (2022). Political fallout in cybercrime circles upping the threat to Western targets. Cyberscoop. https://www.cyberscoop.com/russia-ukraine-cybercrime-ransomware-threat/ (accessed 16 June 2022).

Villadsen, Ole (2022). Unprecedented Shift: The Trickbot Group is Systematically Attacking Ukraine. Security Intelligence, 7 July 2022. https://securityintelligence.com/posts/trickbot-group-systematically-attacking-ukraine/ (accessed 17 January 2023).

Vu, V., Daniel R. Thomas, Ben Collier, Alice Hutchings, Richard Clayton & Ross Anderson (2022). Getting Bored of Cyberwar: Exploring the Role of the Cyber Underground in the Russia-Ukraine Conflict. Manuscript under review. https://arxiv.org/abs/2208.10629 (accessed 17 January 2023).

Wahl, Thomas (2021). E-Evidence Package: EP Paves Way for Trilogue Negotiations. EUCRIM News, 19 January 2021. https://eucrim.eu/news/e-evidence-package-ep-paves-way-trilogue-negotiations/ (accessed 13 August 2022).

Wahl, Thomas (2020). 25 Organisations Demand Fundamental Rights-Based Approach to E-Evidence Legislation. EUCRIM News, 28 December 2020. https://eucrim.eu/news/25-organisations-demand-fundamental-rights-based-approach-e-evidence-legislation/ (accessed 13 August 2022).

Walker, Summer (2019). Cyber-Insecurities? A Guide to the UN Cybercrime Debate. Global Initiative Against Transnational Organized Crime. https://globalinitiative.net/wp-content/uploads/2019/03/TGIATOC-Report-Cybercrime-in-the-UN-01Mar1510-Web.pdf (accessed 13 August 2021).

Warrell, Helen (2021). GCHQ to use new cyber force to hunt ransomware gangs. Financial Times. https://www.ft.com/content/2e391872-428d-44bf-8910-23f123c8aaa6 (accessed 16 June 2022).

Webber, Craig & Yip, Michael (2018). The Rise of Chinese Cyber Warriors. International Journal of Cyber Criminology 12 (1): 230–254.

Weber, Valentin (2022). Financial Incentives May Explain the Perceived Lack of Ransomware in Russia's Latest Assault on Ukraine. https://dgap.org/de/forschung/publikationen/financial-incentives-may-explain-perceived-lack-ransomware-russias-latest (accessed 11 January 2023).

Williams, Brad D. (2021). Proposed 'Hack-Back' Bill Tells DHS To Study Allowing Companies To Retaliate. Breaking defense, 23 July 2021, https://breakingdefense.com/2021/07/proposed-hack-back-bill-tells-dhs-to-study-allowing-companies-to-retaliate/ (accessed 5 August 2021).

Windle, James & Graham Farrell (2012). Popping the Balloon Effect: Assessing Drug Law Enforcement in Terms of Displacement, Diffusion, and the Containment Hypothesis. Substance Use & Misuse 47 (8–9): 868–76.

Wong, Arthur (2020). Why Cybercrime Spikes Around Major Events And Unrest. Forbes, 23 September 2020. https://www.forbes.com/sites/forbestechcouncil/2020/09/23/why-cybercrime-spikes-around-major-events-and-unrest/?sh=7958e0ba6ebe (accessed 23 September 2021).

World Economic Forum (2020). Partnership against Cybercrime. Insight Report. http://www3.weforum.org/docs/WEF_Partnership_against_Cybercrime_report_2020.pdf (accessed 11 August 2021).

Zettl-Schabath, Kerstin (2022). Turning the Tables on the Attackers: How to Hack the Hackers' Supply Chains. https://strapi.eurepoc.eu/uploads/Turning_the_tables_on_the_attackers_Spotlight_article_Nov_2022_682e080772.pdf?updated_at=2022-12-01T15:06:52.281Z (accessed 19 .(January 2023

ABOUT THE AUTHORS

Mischa Hansel leads IFSH's research on "International Cybersecurity". He is a political scientist by training. *hansel@ifsh.de*
Jantje Silomon is part of the "International Cybersecurity" team at IFSH as a Senior Researcher and has a computer science background. *silomon@ifsh.de*

ABOUT THE PROJECT

The work of IFSH's "International Cybersecurity" research area focusses on how escalations in cyberspace can be avoided or conflict regulated, bringing together different political and technical approaches. It is funded by the German Federal Foreign Office.

Funded by:
Federal Foreign Office

ABOUT THE INSTITUTE

The Institute for Peace Research and Security Policy (IFSH) researches the conditions for peace and security in Germany, Europe and beyond. The IFSH conducts its research independently. It is funded by the Free and Hanseatic City of Hamburg.

Funded by:
Hamburg | Ministry of Science, Research, Equalities and Districts

DOI: https://doi.org/10.25592/ifsh-research-report-012

IFSH – **Institute for Peace Research and Security Policy** at the University of Hamburg
Beim Schlump 83 20144 Hamburg Germany Phone +49 40 866077 - 0 ifsh@ifsh.de www.ifsh.de