Spotlight Article

April 2023

European Repository of Cyber Incidents

One Year of Hostilities in Ukraine: Nine Notes on Cyber Operations

Kerstin Zettl-Schabath, Heidelberg University
Sebastian Harnisch, Heidelberg University

The Russian Federation and its proxies have conducted numerous cyber operations against Ukraine and states supporting its right to self-determination. These and earlier operations have resulted in serious damage and upheaval in Ukraine and elsewhere since 2014. However, many observers feared even more effective Russian attacks against critical infrastructure or integrated conventional-cyber military operations in the wake of the Russian invasion in February 2022. A year into the conflict, a protracted debate continues as to why Russian cyber operations did not meet these expectations, focusing on whether most operations had been successfully thwarted by Ukrainian cyber defences and assisting actors or whether Russian state and non-state actors have been unable or unwilling to widely deploy cyber operations. In contrast, this spotlight article provides nine observations on cyber conflict patterns during the first year of hostilities, focusing on state-non-state interactions and operational patterns while drawing on EuRepoC data and third-party analyses. The cyber-attacker ecosystem is expected to further diversify in the years to come, likely shaping the upcoming cyber threat landscape, as recently echoed by ENISA`s cyber security threat report for 2030. However, states as cyber defenders should also ramp up their response options towards those multifaceted threats, as discussed in this piece.

By analysing changing motivations, incentives, and tactics in the increasingly blurring criminal vs. political cyber conflict spheres, we identify pertinent cyber conflict trends which will shape, for better or worse, the operational environment to come.

www.eurepoc.eu

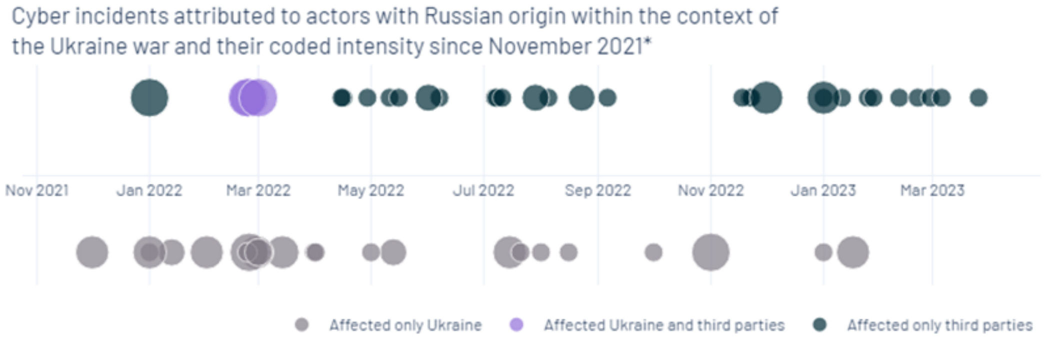
contact@eurepoc.eu

@EuRepoC

1. Cyber operations amounting to the intensity of armed attacks have not taken place in Ukraine.

- Before 24 February 2022, various experts expected unseen levels of offensive Russian operations directly supporting conventional warfare in Ukraine. Instead, what is detectable is an ebb-and-flow pattern of very intense cyber-attacks in the first month of military operations, mostly wiper-operations against Ukrainian targets such as government entities or telecommunication networks, followed by less intense operations since then (see chart below). A joint report by Google and Mandiant (February 2023) states that more disruptive operations took place in the first four months of the war than in the eight years before (i.e., since the annexation of Crimea in 2014), with a culmination around the time of invasion in February 2022.
- Identifying operation types, Russia and its proxies concentrated their activities on disinformation and espionage, presumably to inform conventional warfare and occupational forces, complemented by some attempts to destruct critical infrastructure. Notably, most Russian operations were directed at non-military objectives and major physical disruptions were the exception rather than the rule. In particular, the Viasat satellite hack one hour before the invasion is still the most impactful Russian cyber operation so far, the purpose of which was to disrupt Ukrainian military communication that relied on the KA-SAT satellite. Alternatively, the Viasat hack could have been an auxiliary attack in a wider information warfare/command-and-control warfare operation to increase Ukrainian dependency on more vulnerable land-line communications.
- Russian disinformation and espionage operations have largely fitted into the pre-existing Russian information warfare pattern of targeting Ukraine, NATO, and EU countries. Effective joint conventional-cyber operations have been very rare, contrary to some industry reporting. The concomitance of digital and conventional military strikes is an insufficient indicator of joint operational thinking and capacity. Instead, inconsistent Russian cyber operational patterns suggest that cyber operations have most likely not been coordinated with conventional warfare before 24 February. Moreover, Russian operators have underestimated Ukraine's cyber defences and the effective support it has received. Despite the difficult situation of Russian conventional forces on several fronts, the decreasing number of cyber operations since July 2022 suggests some "operational fatigue" that may or may not be explained by the limited number of capable cyber operators in federal security (FSB), intelligence (SVR) and military (GRU) agencies, the limited use of cyber proxies for coordinated cyber operations, the loss of IT personnel from emigration, or a temporary reorientation/preparatory phase for upcoming attacks (see graph below).

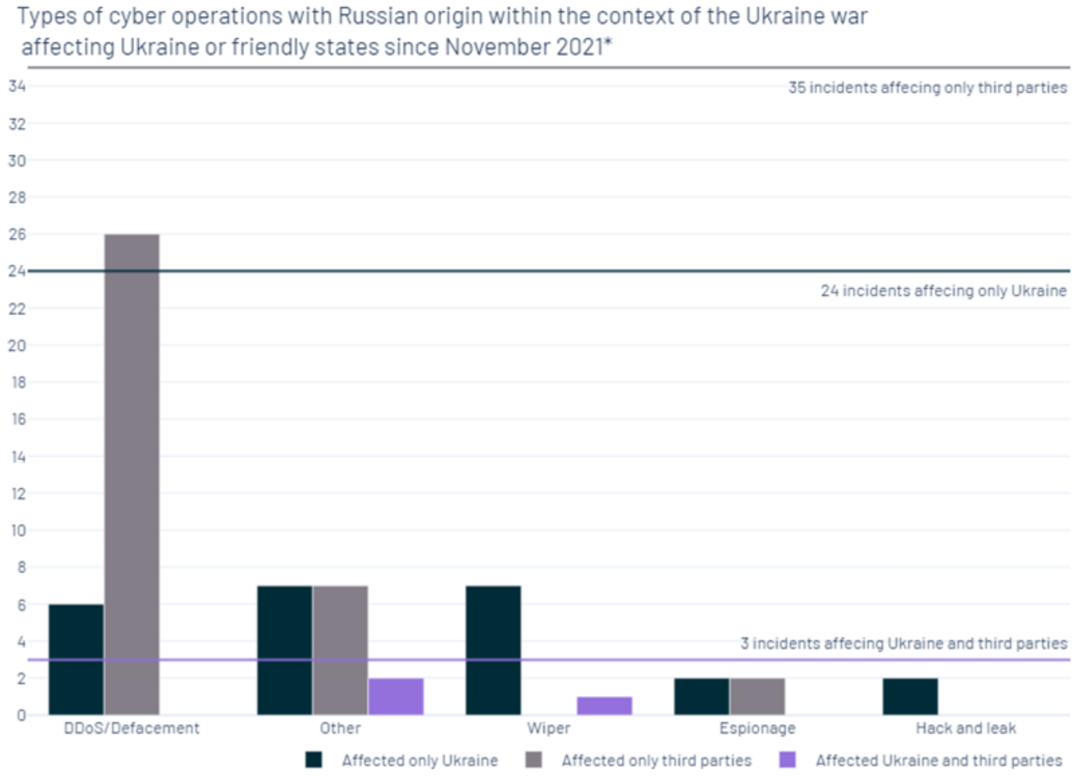
- Thus far, to our knowledge, no government (including Ukraine and Russia) has claimed that cyber operations in Ukraine or related incidents in third states have amounted to an illegitimate "use of force," violating the use of force prohibition in Article 2 (4) of the UN Charter and customary international law. Rather, circumstantial evidence suggests that governments have been hesitant (or uninterested) to suggest that the "use-of-force threshold" has been crossed. However, Victor Zhora, chief digital transformation officer at the State Service of Special Communication and Information Protection (SSSCIP) of Ukraine, argued in January that Russian cyber attacks conducted in coordination with kinetic strikes against Ukrainian civilians could also be classified as war crimes. For this argument to be valid, the claimed "coordination" between kinetic and cyber attacks would need to be backed up by technical analysis that not only points to temporal concomitance as evidence. Apart from an overall consensus that states should uphold not only certain norms of responsible state-behaviour, but also international law in cyber-space, less effort has been made regarding the actual implementation and application of those principles in terms of real-world examples. Varying incentives for using secrecy and obfuscation on both sides of cyber-conflicts might contribute to this "norm acceptance vs. norm implementation" gap, also within the Ukraine war context.[I]



Sample: Incidents with Russian origin since November 2021 within the context of the Ukraine war based on the settled attribution. | The graph displays 62 incidents. Each bubble indicates an incident, their colour indicates the third-party affection, and their size indicates the weighted cyber intensity | * referencing the start date of the incident. Source: EuRepoC 1.0 dataset as of 17.04.2023 - DOI 10.5281/zenodo.7848941

2. Russian actors have effectively used cyber operations as a political, but not military, tool.

- EuRepoC data shows that the overwhelming majority of Russian cyber operations against Ukrainian targets, or those which were attributed to actors that pledged "allegiance" to the Kremlin, were espionage or low level "nuisance" activities. These operations include disinformation, such as DDoS in conjunction with defacements or hack-and-leak operations (see chart below). Russian state actors conducted several offensive operations against critical infrastructure targets, but Ukrainian and/or assisting corporate defenders were able to either thwart the operations or recover the system promptly. Some IT security companies assisting Ukrainian authorities, such as Microsoft, reported a substantial number of successful Russian cyber operations in close coordination with conventional operations. Such findings cannot be confirmed by EuRepoC data and analysis. To begin with, data on the reported coordinated operations by Russian forces is not detailed or abundant enough to prove the suggested sophistication of integrated warfare, which also applies to combined, joint, and virtual manoeuvre contexts. Second, if Russian forces were capable of integrated warfare, including cyber operations, they should have shown this capacity particularly during critical phases of the Russian conventional operations, which they have not. Third, given that Russian actors should be able to improve their operational sophistication over time, current Russian cyber operations indicate that sophistication did not improve and that it fares relatively poorly when compared to improved conventional operations, particularly after partial mobilisation in September 2022. The lack of successful synchronisation between Russian cyber and conventional military attacks was most recently emphasised by a joint report from the Dutch General Intelligence and Security Service (AIVD) and the Military Intelligence and Security Service (MIVD). The report also highlighted the proficiency of Ukrainian defence efforts in conjunction with support by Western allies.

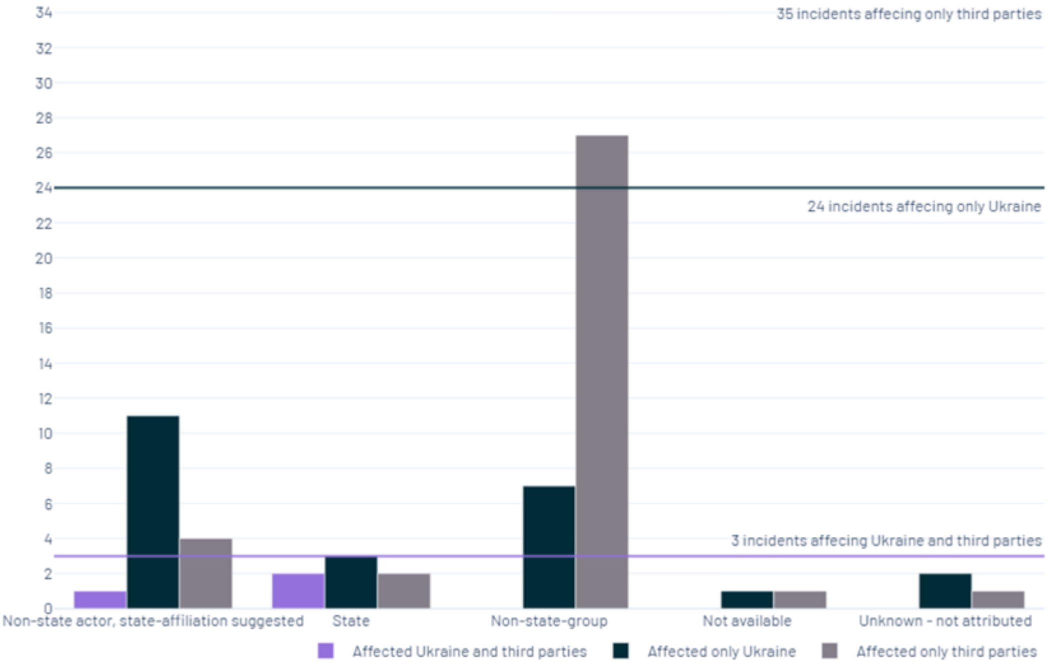

Types of cyber operations with Russian origin within the context of the Ukraine war affecting Ukraine or friendly states since November 2021*

Sample: Incidents with Russian origin since November 2021 within the context of the Ukraine war based on the settled attribution. The graphic displays the count of coded operation types differentiated by third party affection out of 62 incidents in the dataset. | * referencing the start date of the incident. | Operation Type is determined by Incident type combinations: DDoS/Defacement (Disruption without Hijacking), Hack and leak (Data theft & Doxing), Wiper (Disruption and Hijacking with Misuse), Espionage (Data theft), Other: (other combinations). | Source: EuRepoC 1.0 dataset as of 17.04.2023 - DOI 10.5281/zenodo.7848941

3. Russian authorities have been able to muster up non-state cyber actors, state-led APTs, ransomware-groups, and hacktivists to intensify cyber operations in Ukraine (see chart below). However, resulting operations do not show new patterns of operational coordination, nor do target patterns or choice of methods show significant deviations from previous years.

- A year into the war, Russian government proxies have not been able to execute more destructive operations than before hostilities ensued on 24 February 2022. Rather, the intensity and frequency of cyber operations has levelled out after an early hiatus in March/April 2022. Specifically, state-integrated APTs, such as APT28, still focus on espionage, while cyber-crime groups which pledged allegiance to the Kremlin stick to ransomware attacks. In turn, Russian patriotic hackers, such as Killnet, still concentrate on DDoS and defacement activities, which are sometimes called "nuisances" (please also see note 5). Overall, these groups have not been able to substitute for Russia's weak cyber defence, resulting in a rise of attacks against Russia's IT systems after hostilities ensued.
- Moreover, Russia's non-state cyber capacities appear to be outmatched both in defensive and offensive operations when compared to the IT Army of Ukraine, other hacktivist groups/collectives with no reported state-affiliation, such as Anonymous, and corporate actors assisting Ukraine, such as Microsoft. It stands to reason that the brain-drain in Russia's IT sector, in combination with Western sanctions, will further tilt the balance of non-state cyber forces assisting both parties in Ukraine's favor.

Initiator type of cyber operations with Russian origin within the context of the Ukraine war affecting Ukraine or friendly states since November 2021*



Sample: Incidents with Russian origin since November 2021 within the context of the Ukraine war based on the settled attribution. The graphic displays the count of coded operations differentiated by initiator type and third-party affection out of 62 incidents in the dataset. | * referencing the start date of the incident. Source. EuRepoC 1.0 dataset as of 17.04.2023 - DOI 10.5281/zenodo.7848941

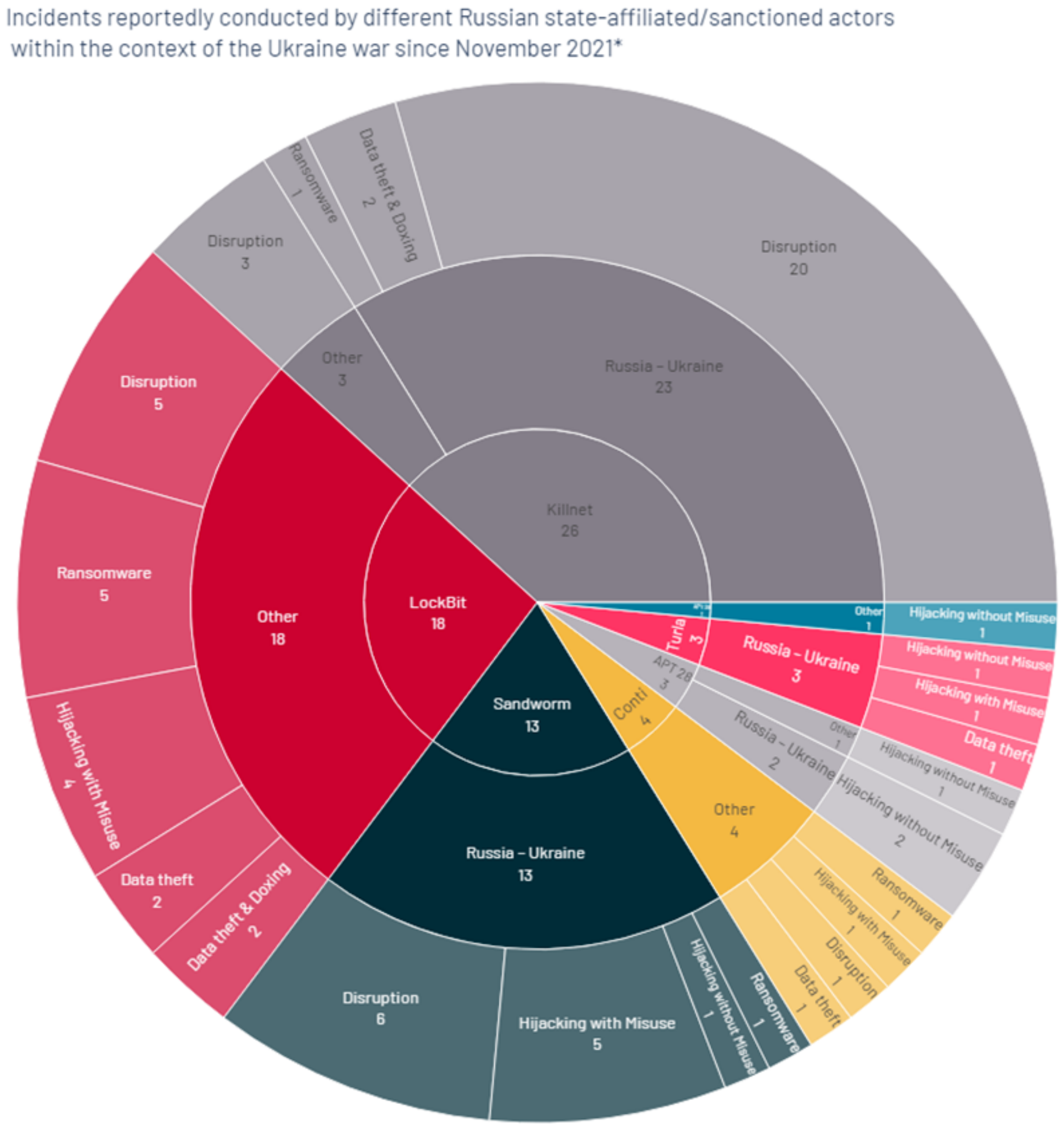
4. The “brain-drain” from Russia`s technology sector and forced recruiting of IT experts since September 2022, e.g., from prisons, presages a potential regrouping of Russian state cyber units and cyber-crime groups in the Commonwealth of Independent States.

- Recently, various threat intelligence reports suggest that the composition of cyber-crime groups has changed over political allegiance questions. After the Conti ransomware group pledged its loyalty to the Kremlin in the wake of the invasion, an internal rift occurred between the pro-Russian and pro-Ukrainian members. But other ransomware gangs, like LockBit or ALPHV (BlackCat) have reportedly avoided taking sides in the conflict, prioritising shared economic interests among the groups' members over potentially diverging national-patriotic sentiments.
- As of the end of March 2023, there are few indications that the regrouping among operation personnel in Russian state units has resulted in dramatic changes in tactics, techniques, and procedures (TTPs), e.g., use of malware.

5. When compared to covert espionage operations by “classic” Russian APTs such as Sandworm or APT28, ransomware groups with Russian ties, e.g., Conti, strongly dominated public cyber conflict reporting.

- Russia’s most prominent APTs, sometimes called the “fabulous four” (Sandworm, Turla, APT28, and APT29), did not markedly change their operational pattern targeting Ukraine after hostilities ensued. They maintained their usual business (see graph below), e.g., political spying against NATO members which, of course, would now involve much more Ukraine-related information. For example, APT28 gained access to a US satellite communications provider in 2022, highlighting the increased salience and strategic importance of satellite networks as targets of cyber-attacks. In turn, GRU-affiliated APT Sandworm held on to its (more) disruptive operational profile when conducting several wiper attacks against Ukrainian targets (examples: CaddyWiper, NikoWiper), but did not cause major havoc. Notably, none of the above-mentioned APTs was responsible for “one decisive cyber-strike” that could have changed the course of the war in favor of Russia. Proxies focusing on espionage, such as Turla, also targeted Ukrainian organisations in the run-up to the invasion, using malware ANDROMEDA since December 2021.
- Operational patterns of ransomware outlets, such as Conti or LockBit, disrupted different sectors worldwide, causing a state of emergency in Costa Rica in May 2022, but showed little coordinated or functionally-specified campaigns vis-à-vis Ukrainian targets.

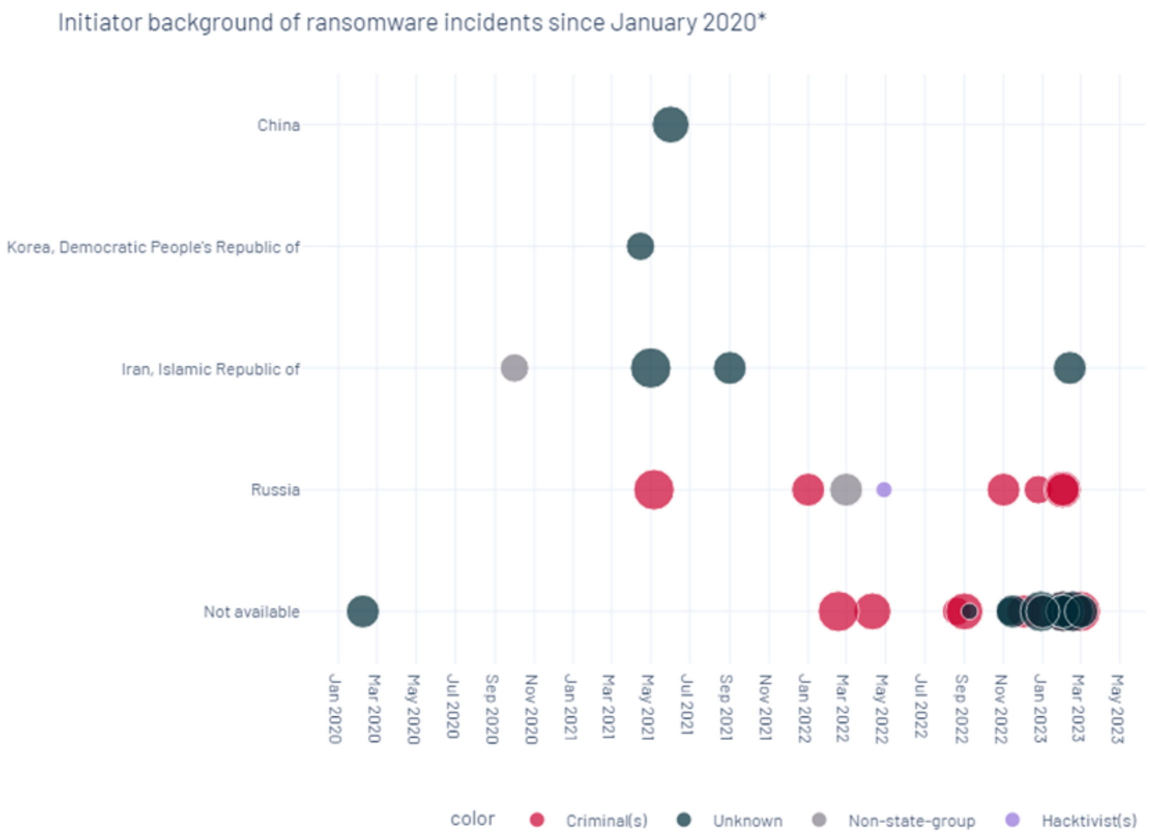
- Hybrid actors which do not exclusively focus on hacking or disinformation campaigns because they combine both within their campaigns, such as Ghostwriter, require more attention by state actors, according to a report by Cardiff University. The authors argue that state agencies strictly-divided responsibilities for countering hacking or disinformation leaves them blind for the combination of both operational types, i.e., “linkage blindness.”


Incidents reportedly conducted by different Russian state-affiliated/sanctioned actors within the context of the Ukraine war since November 2021*

Sample: Incident types conducted by Russian state-affiliated/sanctioned actors since November 2021 based on settled attribution. The graphic displays 68 incident types coded for 40 incidents in total, broken down by the share of each actor in the inner pie, the share of the offline conflict in the middle pie, and the share and count of specific incident types for each actor in the outer pie. Note that each incident can have multiple incident types. | * referencing the start date of the incident. | Source: EuRepoC 1.0 dataset as of 17.04.2023 - DOI 10.5281/zenodo.7848941

6. (Russian) ransomware campaigns increasingly developed into a hybrid form of operation, blending financially motivated money-raising and politically motivated disruption.

- The frequency of ransomware operations decreased in 2022 compared to 2021 according to various reports, while average payouts per operation increased, resulting in attack patterns focusing on high-level targets such as critical infrastructures, with special focus on the health, manufacturing, and energy sectors. But strong regulatory attention to ransomware operations, in combination with several sanction packages against Russian actors, set strong disincentives for many victims to pay the ransom.
- From an operational point of view, criminal motivations for "quick cash" were sometimes blended with geopolitical considerations of hosting governments, such as through targeting critical infrastructure entities of rival states. This is also reflected by the proportion of ransomware attacks attributed to Russian-based/affiliated cyber criminals frequently targeting political/state entities and/or critical infrastructures since 2022 and have therefore been included in the EuRepoC database (see below). A different view of these ransomware operations attributed to states or their proxies interprets them as individual moonlighting activities without state orders.
- From a political perspective, attributing highly-disruptive ransomware operations during hostilities could be even more important than in peace time because escalation dynamics need to be calibrated more carefully. Given that cryptocurrency thefts still generate much higher returns than ransomware attacks, the former should be more prevalent than the latter during peacetime. However, when ransom operations are motivated by both economic and political goals, they may constitute the "tool of choice" because the ransom extracted can also be used to fund further cyber operations, thereby creating a self-sufficient system.
- Against this backdrop, several Western states stepped up their efforts to counter ransomware operations in 2022. Countermeasures include indictments, arrests, diplomatic pressure on ransomware-gang-hosting states, but also increasingly (joint) law enforcement actions, such as botnet takedowns or sanctions against cryptocurrency mixers. Beyond the United States, allied countries, such as the UK and South Korea, recently embarked on this policy course as well.

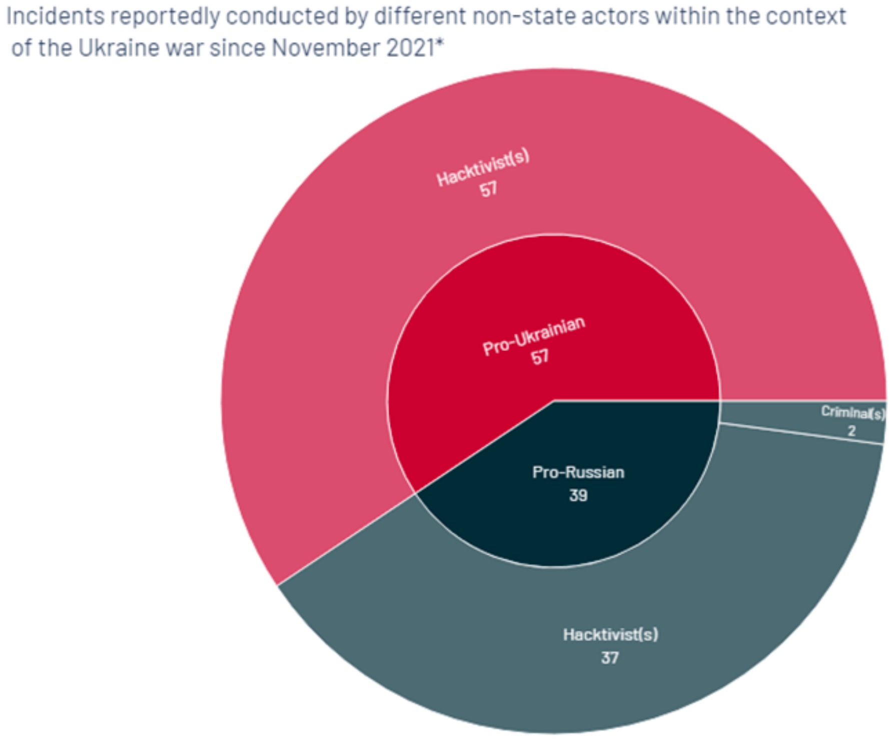

Initiator background of ransomware incidents since January 2020*

Sample: Incidents of type "Ransomware" since January 2020. | The graphic displays 43 incidents in total broken down by the share of each initiator type and country of origin. Each bubble indicates an incident, the colour indicates the initiator type, and the size indicates the weighted cyber intensity. | * referencing the start date of the incident. | Source: EuRepoC 1.0 dataset as of 17.04.2023 - DOI 10.5281/zenodo.7848941

7. When addressing potential legal consequences of "cyber vigilantism," states engage in a variety of practices.

- From the start of hostilities, Ukraine's government proactively and openly recruited hackers for its "IT Army." Through their recruitment and coordination, these groups may be deemed as being "under effective control" of the Ukrainian Ministry of Digital Transformation. In turn, while their members should not be considered as "combatants" in the international armed conflict, the Ukrainian government (and others knowingly hosting them) may be held legally accountable for (some) of their actions.[II]
- In turn, the Russian government recently stated plans to exempt patriotically-acting hacktivists at home and abroad from punishment, indicating that it is trying to form a transnational coalition of hackers similar to the IT Army of Ukraine. (The graph below illustrates the proportions of pro-Ukrainian vs. pro-Russian non-state cyber-attacks recorded by EuRepoC since November 2021.)

- While state practice evolves (e.g., most recently, Belgium was the first European country to introduce its own safe harbor framework for ethical hackers), various questions remain open regarding the concrete status of different non-state actors in roles vis-à-vis state parties involved in international armed conflict and how accepted principles of international law, such as due diligence, have a bearing on the state and nonstate actors' legal responsibilities.



Sample: Incidents conducted by non-state actors within the context of the Ukraine war since November 2021. | The graphic displays 96 incidents broken down by share/count of the faction in whose favour the incident occurred in the inner pie and the share/count of the type of actor in the outer pie. Faction is determined by the initiator country according to settled attribution and the receiver country: Russian or Belarusian Actors targeting Ukraine or friendly states (Pro-Russian); Ukrainian pro-Russian actors targeting Ukraine or friendly states (Pro-Russian); Ukrainian or friendly actors targeting Russia or Belarus (Pro-Ukrainian); or Russian/Belarussian Pro-Ukrainian actors targeting Russia or Belarus (Pro-Ukrainian). | * referencing the start date of the incident. | Source: EuRepoC 1.0 dataset as of 17.04.2023 - DOI 10.5281/zenodo.7848941

8. Cyber assistance by third parties, most notably the United States, Britain, and EU-member states, is an important new policy pattern during hostilities in Ukraine.

- Ukraine has been remarkably successful in mobilising international cyber assistance from states, technology companies, and private researchers, which can be seen as a special form of "cyber soft power." The cyber assistance for Ukraine plays out along two pathways: through third-party state agencies directly supporting Ukrainian authorities in defending their networks and, indirectly, by way of Western states hosting corporate actors protecting Ukrainian governmental data, websites, and networks, triggering the question whether cyber assistance below the threshold of co-belligerency results in an identifiable Russian response.

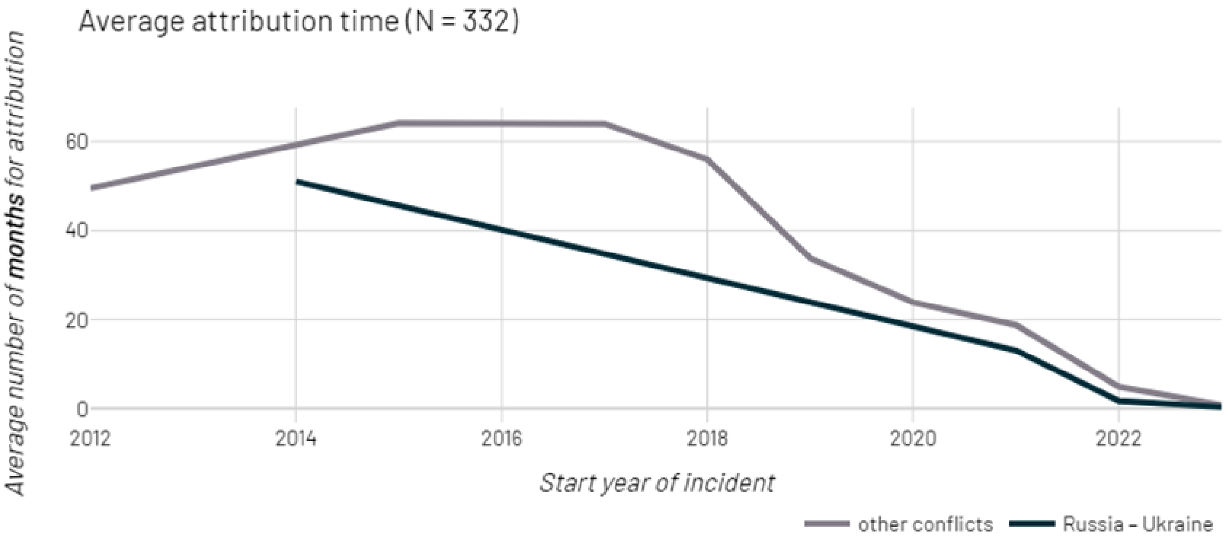
- While it is difficult to dissect the effects of conventional weapons transfers by EU and NATO countries to Ukraine from cyber assistance, it is plausible to suggest that the effects of the latter have been moderate or low. Specifically, Google's TAG has picked up an increase in phishing attacks against NATO countries by 300% in 2022 compared to 2020, most of it from a Belarusian government-backed group called PUSHCHA. However, it remains unclear if this geopolitical information-gathering behaviour, e.g., against Polish government or military organisations, is directly tied to Poland's weapons transfers to Ukraine, or if it represents a regular intelligence-collection effort related to other dimensions of the conflict, such as the monitoring of Ukrainian refugees.

Notably, on several occasions, we detected that a specific policy decision by an assisting country or entity, Poland, the EU, and Germany, appears to have triggered a (low level) cyber response by pro-Russian hackers (see below for examples). On 27 October 2022, a concerted DDoS attack hit the Polish Parliament one day after it passed a resolution calling the Russian government a "terrorist regime." In a similar vein, in late November 2022, the European Parliament faced a DDoS attack after voting to declare Russia "a state sponsor of terrorism." There is some indication that these "loud and short operations" regularly draw more public attention than, for example, more impactful attacks against critical infrastructure. As a consequence, public perception of cyber conflict dynamics in assisting countries may be skewed in favor of the attacker who seeks maximum political effect with minimum technical effort.

Policy Events/Decisions			Reaction(s) in Cyber-Space
	2022		
Poland becomes "logistical hub" for weapons supply in Ukraine	02/03	03	Russian state-sponsored hacking group IRIDIUM uses new Prestige ransomware to attack transport and logistics companies in Ukraine and Poland
Marcel Ciolacu, President of the Romanian Chamber of Deputies, reportedly promises Ukraine "maximum assistance" in the supply of lethal weapons	04	29.04	Pro-Russian group Killnet attacks Romanian websites from the state and private sector
Lithuania bans the transit of goods through their territory to the Russian exclave of Kaliningrad due to EU sanctions	06	06	Pro-Russian groups Killnet and NoName057(16) targets Lithuanian corporate and government websites in June 2022
Norway blocks Russian cargo to the Svalbard archipelago; it donates long-range rocket artillery (MLRS) to Ukraine and pushes for NATO membership for Finland and Sweden	06/07	29.07	Pro-Russian group NoName057(16) targets Norwegian government websites with DDoS attacks
Former Minister of Defence of Moldova, Anatol Salaru, criticises Vladimir Putin and Russia's aggression against Ukraine	08	23.08	Pro-Russian group Killnet targets Moldovan public and corporate websites
Poland passes a resolution that designates Russia a "terrorist regime"	26.10	27.10	A concerted DDoS attack hits the Polish Parliament
Starlink continues financing satellite internet in Ukraine	10	18.11	Pro-Russian group Killnet claims DDoS attack against US-company Starlink
European Parliament designates Russia a state sponsor of terrorism	23.11	23.11	Pro-Russian group Killnet takes down the European Parliament website with a DDoS attack
	2023		
Germany announces that it will send Leopard tanks to Ukraine	25.01	25.01	Pro-Russian hacktivists group Killnet disrupts the websites of German private and state entitites
Italian Prime Minister Giorgia Meloni visits Kiev	21.02	21.02	Pro-Russian collective NoName057 conducts DDoS attacks against websites of Italian companies and institutions

9. Noticeably, the average time gap between cyber operation onset and (public) attribution is shrinking, according to EuRepoC data (see below).

- What holds true for general cyber operations also applies to cyber incidents during hostilities in Ukraine: public knowledge and reporting about cyber operations is always a preliminary snapshot in time. As covert operations seeking non-detection over time, cyber operations are meant to stay in the shadows for long time periods. Beyond the so-called "dwell time" for cyber operations, i.e., the period between initial access to the target networks and the time that the unauthorised access is noticed by the victim or third-party actors (e.g., IT companies), the average time between the start date and the public attribution of an operation has shrunken considerably (see below).
- From a threat-hunting perspective, the initiation-attribution gap can be deliberately shaped by the victim, e.g., by monitoring the attacker in the penetrated system without blocking access immediately. If so, the target decides to extend the time gap between the mean time to detect (MTTD; the moment the intruder is detected) and the mean time to respond (MTTR; the moment a target reacts to this intrusion). In many of these cases, the strategic decision to delay attribution remains unknown to the public, which, in turn, can affect the understanding of detection, attribution, and ultimately cyber incident response patterns.



Sample: All incidents coded on the basis of the EuRepoC framework since March 2022 that have been attributed to an attacker. | The graph displays the number of months between the reported start and attribution dates of 332 total incidents. The graph differentiates between incidents that are related to the war against Ukraine and other incidents. | Source: EuRepoC 1.0 dataset as of 17.04.2023 - DOI 10.5281/zenodo.7848941

[I] Consider the alleged case of a cyber operation by the Main Intelligence Directorate of the Ministry of Defense of Ukraine (GURMO) against a Rosneft oil facility in Belgorod, exclusively reported by one US cyber expert, but not echoed by other major news outlets or cyber threat intelligence companies. For context, GURMO operations have been reported by US cyber expert Jeffrey Carr, who, in turn, claims to have been helping GURMO with fundraising for a planned OSINT platform to track Russian terrorists in the region before 24 February 2022. Then, on April 5, Carr published an article about an alleged offensive cyber sabotage operation by GURMO against several Russian oil facilities, including the one operated by Rosneft in Belgorod. Reportedly, on April 1, a fire had occurred at this oil depot, with Russian officials blaming Ukrainian helicopter attacks for the destruction and Ukrainian authorities eventually denying the claim. In the aftermath, however, the governor of Belgorod claimed that two workers were injured. It follows that if an GURMO cyber operation had (directly) caused a fire at the oil facility, as claimed by Carr, and if the fire had resulted in physical harm to two workers, as claimed by the governor of Belgorod, then that operation may have crossed the use of force threshold. But given that Carr's claims have received little attention and have not been picked up by Russian media or Russian officials, it is plausible to conclude that either Carr's claims are deemed not credible or have been (purposefully) neglected. In the latter case, and given that Russian authorities have not shied away from accusing Ukraine of attacking Russian territory in the past, it is fair to suggest that the deliberate neglect of a (successful) Ukrainian cyber operation against critical Russian infrastructure may reflect the intention by Russian authorities to forego the reputational costs and implications of the attack. By keeping the attack and its impact obscure and/or secret, Russian authorities may want to downplay the domestic costs of the aggression in Ukraine while avoiding calls for an escalation of cyber operations against Ukraine which in turn may result in more Ukrainian cyber-attacks, revealing Russia's weak cyber defenses. This episode further strengthens the importance of incorporating the concepts of "secrecy" and "obfuscation" into cyber-conflict theory-building, since the (non-)disclosure of cyber-attacks as a whole or certain aspects of it can be a deliberate choice by policy makers and security agencies, on part of both the attackers and targets.

[II] After the pro-Ukrainian hacktivist group NB65 claimed that it had shut down the control center of Russia's space agency in March, Russia warned that a cyberattack against its satellites would be a justification for war. The incident clearly indicates that non-state actors may, through their actions, escalate interstate conflicts. Russia may hold Ukraine and the third-country hosting the cyber attacker accountable for either coordinating their actions or failing to subdue non-state actors from executing cyber operations amounting to the use of force, as Martin Müller and Sebastian Harnisch discussed here.

Graphs courtesy of Jonas Hemmelskamp.

About the authors:

- **Dr. Kerstin Zettl-Schabath** is a researcher at the Institute of Political Sciences (IPW) at Heidelberg University.
- **Prof. Dr. Sebastian Harnisch** is Professor of International Relations and Foreign Policy at Heidelberg University.
- **Jonas Hemmelskamp** is a political science student and research assistant at the Institute of Political Science (IPW) at Heidelberg University.