GLOBAL INITIATIVE
AGAINST TRANSNATIONAL ORGANIZED CRIME

LAWLESS CYBERSPACE

WHY EASTERN EUROPE LEADS GLOBAL CYBERCRIME

LUKE RODEHEFFER

APRIL 2025

ACKNOWLEDGEMENTS

The author would like to thank the many security researchers and law enforcement professionals who wish to remain anonymous: this project would not have been possible without you.

ABOUT THE AUTHOR

Luke Rodeheffer is an expert on Eastern European cybercrime. He has spent over a decade researching the space on behalf of organizations in the public and private sectors. He has a graduate degree from Stanford, a CISSP certification, and speaks Russian, Turkish and German.

Please direct inquiries to:
The Global Initiative Against Transnational Organized Crime
Avenue de France 23
Geneva, CH-1202
Switzerland
www.globalinitiative.net

CONTENTS

ACRONYMS

ATO	Account takeover
CIS	Commonwealth of Independent States
DDoS	Distributed denial of service
FSB	Russian Federal Security Service
IP	Internet protocol
ISP	Internet service provider
TLS	Transport layer security
USSR	Union of Soviet Socialist Republics
VPN	Virtual private network

EXECUTIVE SUMMARY

Cybercrime continues to proliferate each year, causing trillions of dollars in damage to the global economy and increasing the leverage of organized criminals. Russia, Ukraine and other parts of the former Soviet bloc play host to some of the world's most sophisticated cybercrime.

This report outlines how the region rose to cybercriminal prominence. It then delves into how two years of war between Russia and Ukraine has reshaped major contours in the cybercriminal and hacking landscape, before offering tentative insights into potential longer-term ramifications.

The profound social ruptures triggered by the collapse of the Union of Soviet Socialist Republics (USSR) and Russia's subsequent adoption of an oligarchic economic model – together with Moscow's repeated and intensifying attempts to retrieve parts of its old sphere of influence – are the three standout long-term regional drivers of cybercrime. The collapse of the old system left thousands of mathematically talented individuals rudderless in a society where collective wealth, for all its limitations, was suddenly transferred into the hands of a tiny elite. Little surprise, therefore, that much of this talent went underground and illicitly exploited the many lucrative opportunities unleashed by the internet era.

Hacking supplements the income of thousands of members of the underground in Russian-speaking countries, particularly for individuals with IT skills, where salaries still lag behind the West. A smaller number earn their income exclusively from cybercrime. The community has rapidly developed a division of labour, so that cybercriminals can specialize in one activity: one user is in charge of botnet infections, while another is in charge of spam operations, a third sells logs from the botnet to forum users, and so on. Cybercrime can be performed at any time and the targets can be global, so the opportunities for cybercriminal activity know no geographical boundaries.

The region's extraordinary expertise in information technology and information security, weaknesses in the rule of law, widespread use of shell companies, money laundering and the proliferation of largely unregulated cryptocurrencies are major drivers of today's cybercrime. A refreezing of Russia's relations with Western powers, driven in part by the Russo-Georgian war (2008) and Russia's invasion of and annexation of Crimea from Ukraine (2014) closed the window on the rapprochement of the 1990s and early 2000s. In turn, this nullified multi-polar cooperation on cybercrime at a time when the phenomenon was proliferating into a major international security threat.

Russia's invasion of Ukraine has upped the stakes still further, to the point where a new shadow war between Western powers and Russia is playing out, in part, in the cybersphere. It is characterized by both Moscow and elements close to Kyiv to varying degrees mobilizing – and thereby

amplifying – cybercriminal networks. Some networks also feed off Russia's quest to evade financial sanctions imposed by the United States and European Union, while in Ukraine tens of thousands of cyber scammers focus on defrauding Russian citizens.

The report evaluates the implications of these developments, while also tracing the breakdown in relations between Russian and Ukrainian cyber-crime groups, the increased deployment of wiper malware and attacks on critical national infrastructure. It draws on research from the private sector, law enforcement and trial documents, Russian-language forums and messaging systems, memoirs of Eastern European hackers, and the author's own experience researching the subject.

Ukraine accused Russia of being behind an attack on dozens of official Ukrainian websites, including PrivatBank, in 2022. War between the two countries has reshaped the region's cybercrime landscape. *© Beata Zawrzel/NurPhoto via Getty Images*

Key points

- The war between Russia and Ukraine has driven a wedge between the country's respective cybercriminal communities, with cybercriminals working alongside the states or, in the case of Ukraine, targeting Russian citizens on a mass scale. It remains to be seen whether this split is permanent, given the high levels of anonymity that the cybercriminal underground has operated under.
- The expertise among Russian-speaking countries in information technology, a legacy of Cold War competition, combined with a prolonged transition to oligarchic capitalism and a lack of rule of law created conditions that led to the region dominating global cybercrime.
- Cryptocurrencies have become a multifaceted tool for cybercriminals, facilitating cross-border money laundering and protecting cybercriminal proceeds from economic instability created by the conflict.
- The war has blurred the lines between the military and civilian infrastructure, with hacktivists on both sides targeting civilian infrastructure, breaching and destroying data.
- The war has also blurred the lines between soldier and civilian, with hacktivists working alongside government forces on both sides of the conflict.
- The conflict has expanded the nature of cyberwar. Wiper malware, designed to destroy as much data as possible, is now being used by both sides to attack military and civilian infrastructure alike.
- Ransomware has become the most profitable form of cybercrime for the region's cybercriminal underground, supplanting carding and botnets, which still remain sources of income for hackers.
- Russia has used the wartime conditions and expansion of Ukrainian cybercrime targeting Russians as an excuse to launch a massive increase in internet surveillance and crack down on civilian use of internet encryption.
- Given the expansion of cyber activity and capabilities by both sides of the conflict, cybercrime and state-sponsored hacking emanating from the region with global targets are likely to grow as the conflict winds down.

COLD WAR AND TRANSITION LEGACIES

During the Cold War, the Soviet Union placed a strong emphasis on engineering and technical education to enable it to compete in the technological and arms race with the West. The cultivation of mathematical talent from a young age was a strong point of the system. In the Soviet Union's last decades, competitions and training camps proliferated, ultimately to put at the disposal of the state the most talented students in mathematics and the emerging field of informatics.

The need to maintain high levels of information security during the Cold War led to the creation of leading institutions for information security: the KGB's elite Cryptographic Institute, and the successor Academy of Cryptography, Networking and Informatics, is the alma mater of many leading individuals in Russia's information security scene, including cybersecurity expert Eugene Kaspersky.[1]

This ecosystem persisted in Russia during the transition to capitalism, as the Russian state and private sector actors understood the importance of maintaining a pipeline of talent. Prestigious training academies in Russia such as Kostroma Open continue to meet every summer, drawing the best young talent from around the country. These special training centres expanded further in the 2010s, particularly those sponsored by Russia's Federal Security Service (FSB), which also included 'capture the flag' hacking competitions and ideological indoctrination.[2] Many graduates go on to work for the Ministry of Defence, the FSB, and the information security sector.

Over 100 universities in Russia now offer information security as a field of study.[3] Both information security specialists and sophisticated hackers, including Dmitriy Smilianets (a former hacker and carder), Nikita Kuzmin (the designer of the Gozi bank malware) and Iyla Sachkov (the founder of Group IB, a leading cybersecurity company), studied at these institutes.[4]

A lack of rule of law characterized the rapid transition to capitalism, and the internet spread in the 1990s across the former Soviet Union with very little regulation.[5] The Soviet Union's security apparatus had never been able to achieve the level of surveillance over communications technology that their East German counterparts, the Stasi, had created by the 1980s.[6] The newly independent successor states of the USSR often lacked sufficient resources to monitor or police high-tech crime, and the corpus of laws necessary to prosecute computer crime had not yet been developed. In some cases, it was not created until the 2000s.[7]

Ivan Bakanov, the acting deputy chief of Ukraine's security service, reports on the dismantling in 2019 of a major global cybercrime network, headed by a Ukrainian national. © *Sergei Supinsky/ AFP via Getty Images*

Many technical specialists found themselves unemployed or underemployed for extended periods of time in the 1990s, as inflation, political uncertainty and wrenching economic restructuring pushed them into poverty. At the same time, the world of computers and the internet opened up another world for youth who were eager to escape the grim realities of this period.

As hacker culture began to spread around the region, the internet began to more closely link the post-Soviet space with the rest of the world for a more legitimate reason: IT outsourcing. The region began to capitalize on the rise of IT outsourcing in the 2000s, and by 2022 the IT sector constituted 3.5% of Ukraine's GDP,[8] along with estimates of between 5% and 6.5% of GDP in Belarus[9] and 1.2–3.2% of GDP in Russia.[10] The sector quickly attracted top talent, as IT salaries in Belarus and Ukraine are often several times higher than the average salary in other sectors of the economy.[11]

One of the major pillars of the early internet underground was a global network of enthusiasts who believed that software should be free. Known as 'warez', this network spread across North America and Europe. Russia rapidly became a global centre for the distribution of cracked software, as the legal code lacked penalties for software piracy at the time.

Hacking terms

Carding: Stealing credit card information to perform unauthorized and fraudulent transactions. It developed in the 1990s, and has shifted from copying data on the magnetic stripes and hacking point-of-sale (PoS) terminals to stealing the data directly from computers as more credit card transactions have moved online. Many 'carders' do not steal the information themselves, but purchase credit card information from a myriad of so-called 'card shops' on the cybercriminal underground.

DDoS: Distributed denial of service (DDoS) attacks are used to suspend access to a website for a certain period of time, which disrupts business activity for anyone who relies on a website. DDoS attacks require multiple devices to make a coordinated stream of requests at the target, so botnets became a perfect enabler of such attacks.

Drops: People who are used in receiving money following successful account takeover (ATO) fraud, either in the form of electronic transfers or goods purchased by cybercriminals from hacked accounts. Networks of such drops will often use shell companies as aliases for their activities. These networks often coordinate

activities using online web panels, and recruit members through cybercriminal message boards or spam mail claiming to offer roles to work from home with a shipping company.

VPNs: Virtual private networks (VPNs) are a technology designed to protect the activity of computer network users by creating an encrypted tunnel through the broader internet, shielding much of the data from internet service providers (ISPs) and other actors who could attempt to capture the traffic. The cybercriminal underground has a plethora of VPN services that claim to not keep logs of their customer activity, while maintaining servers in data centres around the world to alter and shield geolocation.

Proxies: Botnet devices infected by malware are not solely for information on victims that access to the computer grants. Cybercriminals can also use infected devices as proxies, routing traffic through the compromised device, which is useful if they need traffic to come from a specific geolocation to bypass authentication systems.

Wiper malware: Wiper malware is designed to destroy as much data as possible on target computer infrastructure. It has become increasingly used in geopolitical conflict as a way to destroy as much data as possible across a computer network and render computer technology unusable.

Initial access brokers: Hackers who specialize in gaining an initial foothold into a network. This access can then be sold on the cybercriminal underground to other cybercriminals who can use it to gain deeper access, including ransomware groups who can buy such accesses to quickly deploy as much ransomware as possible.

Exploits: Errors or vulnerabilities in code, operating systems and platforms that can be weaponized by hackers to make the code not perform as intended by the original developers, such as granting attackers more power over the targeted devices, allowing them to bypass authentication measures, access other areas of a computer network or execute other code remotely.

Zero day exploits: An exploit that has not been publicly disclosed and is unknown to the information security community. Zero days are especially powerful and highly sought after by cybercriminals and nation-states alike, because their first use can be devastating and enable major cyberattacks, such as the 2017 NotPetya attacks. Once an exploit has been disclosed by the developers, it is assigned a number by the National Institute of Standards and Technologies (NIST) in the United States and added to the government organization's databases.

Black market for zero days: Actors who are willing to sell zero-day exploits to cybercriminals and nation-states alike, often charging significant sums for the purchase of an exploit that could enable a devastating initial wave of attacks.

Account takeover: Once a cybercriminal has gained credentials, the next stage entails defeating account security and successfully authenticating onto the victim's account(s). ATO specialists will use specialized tools and configurations to defeat anti-fraud systems and other forms of authentication security, and then use the account access to perform fraudulent transactions or serve as a point of entry for deeper penetration into target computer networks.

Botnet logs: Botnets, or networks of infected computers under the control of cybercriminals, generate log files containing valuable information from the victim's device, such as credentials, bank account information, personally identifiable information, or operating system and configuration details. These logs can then be sold to other cybercriminals who specialize in using the data to perform fraud or account takeover.

Frozen conflict zones: Regions with disputed legal status proliferated after the Soviet Union collapsed due to territorial disputes between newly independent republics. These regions' lack of international recognition makes access for international law enforcement actions difficult, and the regions quickly developed into conduits for organized crime, including cybercrime. These regions include Transnistria in Moldova, South Ossetia and Abkhazia in Georgia, and the regions of eastern Ukraine occupied by Russian forces. ■

Cybercrime in the 1990s focused on pirating illegal software and credit card hacking, with the more organized activity taking place in chat rooms and message boards. A seminal moment in the transition from software piracy to financial fraud came in 2001 with the founding of CarderPlanet by Roman Vega. Based in Odesa, this carding organization served as an archetype for dozens of successor forums that emerged in the 2000s. Skimming technology and the breach of large credit card technology meant that a substantial amount of payment card information was now available to fraudsters. Vega eventually pleaded guilty to the charges and was sentenced to 18 years in prison by the United States in 2013.[12]

Carding only became more widespread as online retailers allowed anyone with a credit card number to make a purchase, and special technology such as proxies and VPNs allowed illicit actors to spoof their geolocation. By the late 1990s, carding was so widespread in the Commonwealth of Independent States (CIS) – a political successor organization to the USSR – that Western retailers often expressed concern about expanding operations into Ukraine, Belarus and Russia.

Some hackers also began to generate income by offering DDoS attacks to anyone who wanted to crash the websites of competitors to eliminate competition or settle business disputes. As millions in the region continued to struggle with newfound poverty, underemployment and the jolting transition to market economies, carders gained access to a glamorous and extravagant lifestyle, purchasing expensive cars, attending VIP nightclubs and jet-setting to luxury resorts around the world.[13] Carding also became a 'gateway drug' for hackers, who learned about electronic payments, internet encryption, anonymity and server infrastructure, allowing them to eventually shift into more sophisticated cybercrime.

Russian-speaking hacking quickly developed a reputation. At a conference dedicated to cybercrime, held in London in 2005, the Director of Information Security at the Russian Ministry of Internal Affairs stated that Russian hackers were already 'the best in the world', acknowledging that 'yesterday's adolescents had outgrown their earlier internet pranks' and were now shifting into serious financial cybercrime.[14] At the same time, the information security space began to rapidly grow in Russia and Belarus, with firms like Kaspersky Labs, Group IB and Dr AV developing large international client bases and becoming outliers in an economy dominated by commodities exports.

The hacking community's rising profile did not go unnoticed by law enforcement: a number of raids against CarderPlanet in the early 2000s, followed by the closing of the English-language carding forum ShadowCrew by an international law enforcement operation in 2004, were seen as major blows to global carding at the time.[15]

Cashing out: turning access into profit

Another factor that has contributed to Eastern Europe's dominance of cybercrime is the widespread use of offshoring and shell companies during the transition to capitalism. The ability to create companies and open bank accounts quickly as part of a drive to make economies conducive to private enterprise has lent itself to opportunities for illicit actors to use such shell structures for money laundering and to cash out of compromised payment systems. Cybercrime forums often offer shell company creation services and guides to laundering money.

One advert seen on Telegram in 2024 offered a service to quickly establish a company in the Republic of Georgia for carders and those seeking to cash out funds. It promised that the equivalent of a limited liability company could be incorporated for only US$100, and ready for business within five hours without any capital requirements. The rise of tourism in Georgia means companies can be established quickly and point-of-sale equipment purchased, which the individuals advertising the services claim can be used to cash-out any type of card information that is received from call centre fraud. These fraudulent companies are generally discarded within two or three weeks and replaced with new shell structures.

Exchange and cash-out services are now also automated through the Telegram platform. They also often offer courier services that will deliver hard currency on demand to customers in major cities in Russia, Ukraine and Belarus.

Entrepreneurs began to develop web payment systems in the 1990s to facilitate secure financial transactions at a time when much of the data moving over the internet was unencrypted, and online retailers were eager to incorporate payment systems that allowed customers to pay instantly with credit card information. One such payment system is WebMoney, which was created in Russia in 1998 in the aftermath of a major currency crisis in the country, as demand for foreign currency skyrocketed following the ruble's decline.[16] WebMoney itself is a legitimate payment platform, and evidence suggests that it remains widely used in Russian-speaking countries. WebMoney, like many other payment platforms, became a means by which payments using stolen credit cards could be made, as registration requirements for accounts were minimal at the time.[17]

Other electronic payment systems were developed to cater to the underground's need for effortless financial flows. One major player was Arthur Budovsky, a Soviet émigré to the United States. After initial run-ins with the law for running an unlicensed digital payment processor, he fled to Costa Rica, renounced American citizenship, and founded a new company, Liberty Reserve, in 2006, which he never registered with the US Department of the Treasury.[18] This enterprise allowed users to buy and redeem digital currency through third-party exchanges under pseudonyms without requiring any identity validation. The system had processed approximately US$8 billion of transfers through 55 million transactions when Budovsky was arrested in 2013. He was eventually sentenced to 20 years in prison in 2016.[19]

The original indictment against Liberty Reserve stated that the case was an 'important step' towards reining in the 'Wild West' of illicit internet banking. Unfortunately, nothing could have prepared law enforcement for the rise of cryptocurrencies, a still largely unregulated sphere that has enabled cybercriminals to shift and disperse liquid funds instantly across digital cyberspace. This asset class – which is also a major tool for Russia in its evasion of wartime sanctions – will be evaluated later in the report.

Other types of cybercrime marketplaces have also fallen to law enforcement operations: Genesis, a marketplace run by Russian-speaking cybercriminals, which sold approximately 80 million compromised credentials and browser cookies from over 1.5 million infected devices from around the globe, was taken down by US law enforcement in April 2023. Genesis sold to initial access brokers and account takeover specialists credentials that could enable access to a network; these assets are generally sold onwards to ransomware groups.[20] The development of new technology to protect payment card information, such as the EMV chip, which generates a unique code for each transaction, has shifted the targeting towards card-not-present transactions and may have made carding more difficult in the long term.

In the immediate term, however, cybercriminals have moved away from using skimming technology to using malware that is capable of 'sniffing' the data from a point of sale terminal, and targeting regions where the chip technology has not been introduced or properly integrated, such as Latin America.[21] Larger credit card marketplaces continue to generate daily revenues exceeding US$100 000, according to one researcher.[22]

Rise of ransomware

Ransomware quickly established itself as the most profitable and destructive arena of cybercrime, and an area that is dominated by the Russian-speaking underground. Studies in 2022 by blockchain intelligence experts found that at least 75% of ransomware revenue had gone to actors linked to the Russian-language underground.[23] Despite takedowns of some organizations, ransomware payments reached US$1.1 billion in 2023, the highest level ever recorded.[24] Predecessors to the first ransomware were developed in the late 1980s, but it did not become a widespread attack method until cryptocurrencies began to gain critical mass in the 2010s.

Some hacking forums were initially opposed to allowing ransomware services to advertise on their platforms, both given the malicious nature of the activity and the potential for such advertisements to make the forums themselves into targets.[25] The amount of money that the operations could generate soon changed administrators' minds, however.[26] The profitability of a successful ransomware attack is much higher than traditional credit card hacking, which also involves layers of intermediaries.

This form of cybercrime is also largely immune to geopolitical fallout. 'There is no reason to think that the ransomware wave will decelerate, as the ransomware organizations are already sanctioned and have not even flinched,' one security researcher noted.[27] 'After a temporary lull, the war [in Ukraine] has not slowed down the campaigns. Many of the organizations now have top-down hierarchies, C-suites and office space.'

St Thomas' hospital in London was among the many National Health Service hospitals affected by a ransomware attack in 2024 reportedly carried out by Russian cybercriminals. *© Vuk Valcic/SOPA Images/ LightRocket via Getty Images*

Exploiting geopolitical 'grey zones'

Web hosting providers catering to the underground have meanwhile exploited unresolved territorial disputes that dot the region. One such example is Transnistria, a narrow region of Eastern Moldova that borders Ukraine and has been occupied by Russian peacekeeping troops since 1992, following disputes over whether the region would remain aligned with Moldova as the USSR collapsed. It is not recognized as an independent state by any country.

Transnistria has relied on its disputed legal status to develop a reputation as a haven for smuggling and other illicit behaviour, including cyber activities out of reach of international law enforcement. Cybercriminals have long taken advantage of its status to use data centres that host malicious activity.[28] The infrastructure controlled by these services has also been used by pro-Russian hacktivists to perform massive DDoS attacks against various targets since Russia's invasion of Ukraine.[29]

The expansion of conflict zones in the post-Soviet space has only cemented a sense of security among criminal elements that they are shielded from international oversight when operating in these regions. Russia relied on organized criminal groups to establish control over Crimea after it annexed this territory in 2014. Crimea and the Russia-occupied Ukrainian regions of Donetsk and Luhansk quickly established themselves as 'grey zones' similar to Transnistria, as cybercriminal elements used the regions' unrecognized international status to allow cybercrime to flourish.

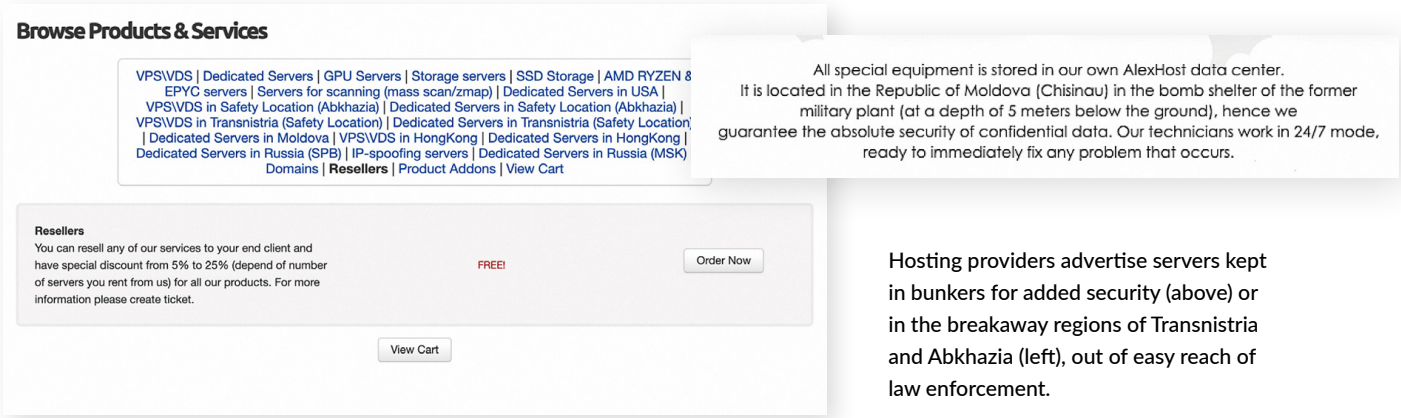
Multiple data centres located in Luhansk are now being used for traffic direction systems, which are pushing generic pharma medicine and adult dating spam, while another data centre sold control of internet protocol (IP) addresses to a shell company in the Seychelles. One data centre moved their IP address space over the course of April 2024 from a location in Luhansk to a company in Venezuela.[30]

Illicit hosting providers do not always rely on shell companies in traditional offshore centres used by post-Soviet states, such as Cyprus, but resort to other offshore jurisdictions, such as Panama, the United Arab Emirates and even the City of London. Some hosting providers even advertise that they keep their servers in underground Soviet-era bunkers as an additional security measure.

While based in Russian-speaking regions, the hosting providers will also often rent IP address space from larger international IT service companies in Western jurisdictions that are less likely to initially arouse suspicion. This also allows these services to offer as many geolocation options as possible.[31] As more organizations have implemented blacklists and actively sought intelligence on hosting services, operators have adopted new technologies, including fast-flux hosting, which involves using bots with different IP addresses to handle requests, making IP-based blacklisting and law enforcement takedowns much more difficult.[32]

In 2019, Ukrainian security services arrested a hacker in Odesa, Mikhail Rytikov, who was accused of involvement in a variety of different cybercriminal activities, including a breach of Nasdaq that caused an estimated US$300 million in damage, the propagation of the Zeus botnet (see the box below) and running a leading hosting provider that catered to the underground. Ukrainian law enforcement claimed that Russian security services used services provided by Rytikov to perform cyberattacks against Ukraine itself and that the provider hosted up to 40% of the Russian-language darknet.[33]

Rytikov had a long history of involvement in cybercriminal activity, from carding to botnet propagation, and was named in an indictment by the US Department of Justice in 2013 for data breach schemes that stole data for over 160 million credit cards.[34] On underground forums, he advertised that his



Hosting providers advertise servers kept in bunkers for added security (above) or in the breakaway regions of Transnistria and Abkhazia (left), out of easy reach of law enforcement.

servers were located in Lebanon and other sites in the Middle East.[35] Rytikov maintained much of the data centre hidden in a basement that contained nearly 150 servers, complete with its own electricity generator. The prosecution of his case by multiple US Attorneys' Offices is still ongoing as of writing, and Rytikov has challenged the accusations in court, claiming that he was merely reselling hosting infrastructure.[36]

Subsequent research indicates that the shell company registered in the Seychelles, which security researchers allege Rytikov had been using to run his hosting service, is again operational, and one of the main data centres that it shares traffic with is located in Luhansk in Russian-occupied eastern Ukraine.[37] The company remains operational as a host for malicious infrastructure, including a penetration testing tool originally developed for defensive teams but that cybercriminals have increasingly appropriated for their own campaigns.[38]

How cybercrime permeates the post-Soviet sphere

Cybercrime in Russian-speaking countries has always had a strong transnational element, relying on the deep ties that continue to connect labour and monetary flows across the post-Soviet space, along with the ability to move money and digital infrastructure across borders easily. Details that emerged in the wake of several takedowns of criminal operations shed light on how cybercrime networks co-operate on a pan-Eurasian basis. Botnets such as GozNym, Kelihos, Zeus and others began to proliferate in the late 2000s and spread rapidly in the 2010s, infecting computers around the world with malware that often sought to steal banking information. These botnets were often administered by cybercriminal organizations that were spread across multiple former Soviet republics. ■

Hackers and the Russian state

The relationship between the hacking underground and the Russian and Ukrainian states has often been shrouded in layers of plausible deniability, but multiple incidents highlight the symbiotic and growing nature of the relationship.

The golden rule of much of the region's cybercriminal community has long been to avoid targeting Russia or other CIS countries, to avoid drawing the ire of the security services, which otherwise ignore some of the activity. This is made explicit in the rules of use listed on Russian-language cybercriminal forums, as well as on advertisements selling malware. Some malware is even designed to detect keyboard settings and stop the execution if it detects settings with Russian or other CIS languages installed.

However, even Russian cybercriminals occasionally break the golden rule and target their own country, treating the Russian Federation as a laboratory for the development of new malware and schemes that are then used globally. Lurk malware, which was developed between 2011 and 2016 and targeted tens of thousands of Russian devices, was one of the first malware campaigns to use fileless infection to target host devices: web banners were placed in strategic locations on websites frequented by financial services employees,[39] and a vulnerability was exploited in the banner system to deploy malware onto devices at banks. Russian law enforcement eventually arrested the group, but not before they stole 3 billion rubles (US$32 million). This file-less technique was quickly adopted by other groups running botnets.[40]

As cybercrime became more sophisticated, Russia's security services began to take notice, shifting from occasional passive collection of income for protection rackets to apparent collaboration to achieve state goals.[41] Russian security services initially depended on Western intelligence on cybercriminal activity in the early 2000s, but began to seek collaboration with the underground around the time of the Russo-Georgian War in 2008, according to several experts interviewed.[42]

In 2020, the US charged six current and former members of Russia's military intelligence agency with allegedly carrying out some of the world's most destructive hacking attacks. *© Andrew Harnik/AP Photo/Bloomberg via Getty Images*

The Russian state also uses hackers it prosecutes to do its bidding in exchange for reduced sentencing, according to hackers interviewed by Russian journalist Daniil Turovskii.[43] This practice is confirmed by other cases: Dmitry Dokuchaev, an FSB information security specialist arrested in Russia and charged with treason in the aftermath of the 2016 US presidential election hacks, was a self-confessed former offensive hacker who specialized in breaching networks and who edited a section of the Russian-language *Hacker* journal dedicated to offensive network activity. He was arrested by the Russian security services in the 2000s and shifted to active cooperation, eventually joining the ranks of the FSB.[44] Russia sentenced Dokuchaev to six years in a maximum-security prison for committing treason on behalf of the US in April 2019 in a trial performed with high levels of secrecy, but he was released before the end of his sentence, in May 2021, for unspecified reasons.[45]

Further relationships between the underground and the state are evidenced by the reuse of malware code sold on the underground by state-sponsored groups. Blackenergy is a piece of malware that was originally marketed on the cybercriminal underground in the late 2000s, before its source code was leaked. The malware underwent subsequent modifications, developing from a regular banking fraud tool to sophisticated software attacks against industrial control systems. A heavily modified version was then deployed by a Russian state-sponsored hacking group to target Ukraine's power-grid in December 2015, leading to massive power outages.[46]

Russian security services also appear to have begun to explore the use of criminal botnets for espionage in the early 2010s. Investigations of the GameOver Zeus botnet, discussed below, found it was probably used for such ends when search commands were found regarding Georgia's and Ukraine's intelligence services, counter-intelligence operations, and Russian mercenaries and militia camps in Syria, according to a 2015 presentation at the BlackHat hacking conference.[47]

The Russian state also relies on the cybercriminal underground to gain unauthorized access to data: two FSB officers were charged by US prosecutors in 2017 with allegedly facilitating and paying cybercriminals to gain access to millions of accounts from Yahoo's user database to enable a spam campaign, and hack into dozens of email accounts. The cybercriminals were identified as Karim Baratov, a Canadian and Kazakhstani national, and Alexsey Belan, a Russian national.[48] Baratov was later sentenced by a US court to five years in prison.[49] Belan remains at large at the time of writing.

The recent arrest of Mikhail Matveev, a ransomware actor, in December 2024 by Russian authorities may be an indication that they are becoming less tolerant of ransomware actors or, at the very least, less tolerant of hackers who are too hungry for publicity: Mikhail Matveev, known as Wazawaka, had given public interviews, including with cybersecurity publications,[50] even after he was indicted by the US Department of Justice in May 2023.[51] Matveev had his cryptocurrency assets confiscated and is currently awaiting trial.[52]

US sanctions Evil Corp

The extensive relationships between the Russian state and the cybercriminal underground are most clearly evidenced by investigations into a group known as Evil Corp, which culminated in the US Department of the Treasury imposing sanctions against this organization in December 2019.[53] This cybercriminal group had deployed Dridex malware, a strand of financial malware that resulted in US$100 million in financial losses, while performing espionage against NATO targets and turning over data to the FSB.[54] Evil Corp targeted several organizations across sectors, including over 300 banks around the globe with banking trojans. One member of the group, Aleksandr Ryzhenkov, allegedly

deployed Bitpaymer, a ransomware variant, against US organizations since 2017, according to an indictment from October 2024 by the US Department of Justice.[55]

The US Department of Justice also announced in December 2019 the unsealing of criminal charges in Pennsylvania and Nebraska against the leader of Evil Corp, Maksim V Yakubets, for his role in deploying the Zeus botnet, and accused him of involvement in financial crime stretching back to at least 2009.[56] The Department of the Treasury claimed that Yakubets 'provides direct assistance to the Russian government's malicious cyber efforts', and was in the process of obtaining clearance to access classified FSB information at the time of the charges. Yakubets' relationship with the Russian security state was not purely financial either: his father-in-law is an FSB special forces veteran who runs a private security company.[57] Yakubets' own father, Viktor Yakubets, was allegedly involved in acquiring the equipment for the group, according to a public report from the US Department of the Treasury.[58]

Despite the increased apparent collaboration, the Kremlin still seeks to maintain some level of plausible deniability in terms of its relationships with the criminal underworld. The Conti ransomware group initially voiced support for Russia's invasion of Ukraine,[59] but withdrew the endorsement only two days later. An expert on state-sponsored hacking noted that this was likely due to Russian security services making it clear to ransomware groups that they should be more discreet.[60]

THE RUSSIA–UKRAINE CYBERWAR

While collaboration between the Russian state and the cybercriminal underground continues, to a greater or lesser degree, the Russia-Ukraine war has led to a split between some cybercriminal groups and communities which had previously collaborated across borders. Higher-profile cybercriminal forums often steer clear of conversations about politics to avoid attracting attention from security services, but in other areas of the Russian-language underground, discussions quickly turned virulent in the aftermath of Russia's invasion. 'Flame wars', or discussions where users insult one another, erupted on lower-tier and entry-level Russian-language forums between supporters and opponents of the invasion, with supporters in some cases labelling their counterparts 'Khokholy', an ethnic slur for Ukrainians, and claiming that they had been brainwashed by American psychological operations.[61]

The most dramatic result of the end of collaboration between the two countries' cybercriminal communities was a leak of chat logs from Conti's private server. One theory behind the leak is that the Ukrainian members of the group were so angry with the invasion that they released the logs to damage their Russian counterparts' operations.[62] Another likely long-term result of the war is a decline in trust between Russian and Ukrainian hackers, who will no longer be willing to share infrastructure, a seasoned researcher of cybercriminal activity noted. Russian cybercriminals already no longer trust Ukrainians enough to collaborate, as they fear incriminating data will be stolen or leaked.[63]

One cybercriminal, speaking on condition of anonymity, noted that they no longer feel comfortable using any service or infrastructure that is under Ukrainian control.[64] Paradoxically, another noted that they avoid any conversation about politics or the war, saying that the less they know about their fellow cybercriminals, the better.[65] Another factor that is likely to have contributed to the split is the war's termination of economic relationships between IT companies that had previously held cross-border contracts.[66]

Previous research conducted by the GI-TOC found that Russian and Ukrainian smuggling networks were continuing to collaborate despite the conflict, as wartime expanded the opportunities for illicit traffic.[67] The decline in law enforcement resources stemming from the war and economic contraction also undermines the ability of local officials to confront the problem. Examinations of communications between cybercriminals do not reveal much in the way of explicit prohibitions on collaboration with other members of the underground based on their nationality. Most cybercriminals' primary concern is earning money, and many actively avoid mentioning their country of origin to prevent their location

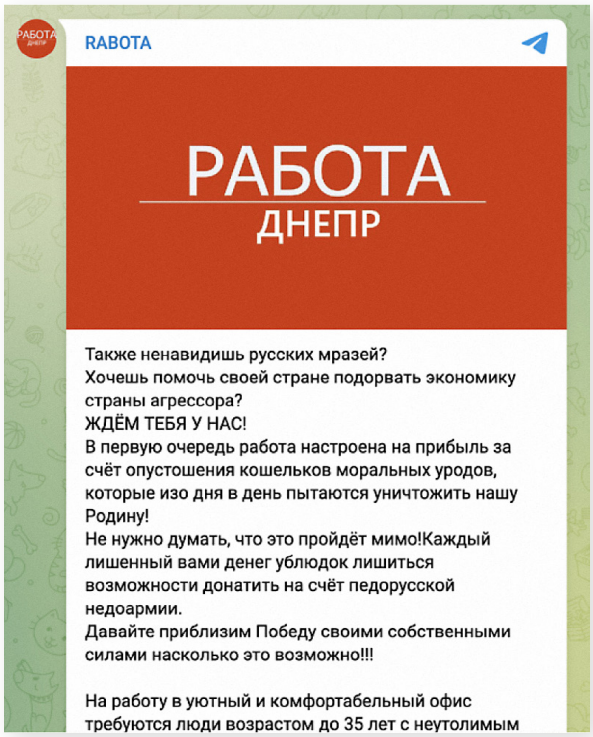
from being determined by researchers or law enforcement. However, overall, there is a marked decline in collaboration between Russian and Ukrainian cybercriminals due to the conflict. Time will tell whether this leads to a permanent split, particularly given that Ukrainian cybercriminals are now increasingly targeting their eastern neighbour.

Ukrainian cybercrime targets Russia

In 2023, Russia experienced a wave of arson attacks against military recruitment and registration offices: in a five-day period between the end of July and the beginning of August 2023, 28 attempts were made to target Russian military barracks with arson attacks, according to independent media reports.[68] These attempted attacks were all linked by a few threads of evidence: the perpetrators were all middle-aged women or pensioners who had been targeted through call centre fraud – a remarkable deception to be revisited later in this section.[69]

Cooperation between Ukrainian and Russian law enforcement, once a regular occurrence, effectively disappeared after the annexation of Crimea and occupation of Donetsk and Luhansk in the 2010s, allowing this type of cybercrime to flourish. Illicit call centres targeting victims with all manner of fraud, from cryptocurrency investment schemes to fake tax preparation centres, have exploded in recent years, including in Russian-speaking countries.[70] The countless databases of personally identifiable information that have been breached and resold on the cybercriminal underground provide a steady supply of new victims.

Call centres that target Russians rely on Ukrainians who can speak and write fluent, accent-less Russian. The following screenshot is a recruitment advertisement circulated on Telegram for a role in the eastern Ukrainian city of Dnipro. It calls for anyone below the age of 35 who 'despises the Russian scum' to 'help their country undermine the aggressor's economy'. The advertisement states that operators can earn over US$1 000 a month while working from a well-furnished office in a picturesque location.



Dnipro is widely considered to be the capital of these call centres. To maintain operations, some of the centres also regularly pay bribes to local police. The centres also maintain ties with traditional organized criminal structures, and in some cases use physical punishment against employees or against journalists attempting to investigate their operations.[71] Estimates for 2023 provided by testimony to Ukraine's parliament put the number of domestic call centres in operation at approximately 2 000, while the local Dnipro press estimates that 120 000 people were employed in such centres as of June 2024.[72]

A call centre in Dnipro seeks Ukrainian recruits fluent in Russian. Dnipro is considered the heart of these scam operations targeting Russians.
Photo: Screenshot from Telelegram

Territory changing hands due to shifting front lines has also provided glimpses into the scale of the cybercrime. When Russian forces began to occupy the Ukrainian city of Berdyansk in 2022, they announced the discovery of a large call centre, located in the city centre, right next to the regional office of the Ukrainian federal security services. This call centre purportedly possessed a database with the personally identifiable information of 20 million Russian citizens.[73]

It is unclear what the success rate of such operations is, but the profitability of successful calls more than compensates for the costs of running the operation: the aforementioned call centre was reportedly generating US$2–3 million in profit every six months.[74]

Typical scams include employees posing as a relative or someone close to the victim and claiming that they are in a dire financial situation. In some cases, scam callers claim to be Russian soldiers on the front who have been injured and are in urgent need of assistance. In other cases, the callers claim to be representatives of the security section of a financial institution used by the victim. The call centre scammers convert cash from victims' bank accounts into cryptocurrency to transfer to the end point in Ukraine.[75]

One of the fraudsters' most startling successes came early in the war. In August 2022, an elderly Russian woman set fire to a car belonging to the Deputy Chief of the Russian General Staff Directorate, believing that it was a Ukrainian espionage asset. She was first told to lend the scammers 1 million rubles (US$11 430), and was then gradually manipulated into more aggressive activities, culminating in the arson attack. Even at the time of her arrest, she had been so successfully socially engineered that she was convinced that she was being apprehended by pro-Ukrainian criminals, not law enforcement.[76]

The scale of the activity led deputies in the Russian Duma to petition the Russian defence ministry in August 2023 to begin considering these call centres 'military objects', allowing them to be targeted by Russian attacks.[77]

An independent estimate by Sberbank, a leading Russian financial institution, calculated that 90% of call centre scams targeting Russians originate from Ukraine.[78] Sberbank also estimates that approximately 3 000 such call centres exist in Ukraine, generating US$1.5–2 billion in revenue yearly. The large number of different cash-out services available on the underground will take a 15–20% commission, and complete the transaction by transferring funds from Russia to accounts under Ukrainian control, often using Russian bank accounts for intermediary transfers.[79]

It is likely that the Russian state's lax attitude toward the sale of data on the cybercriminal underground contributed to the call centre epidemic. Despite the general prohibition on targeting Russia or other nations belonging to the CIS, many users on cybercriminal forums also sometimes sell access to Russian government databases derived from both civilian agencies and those controlled by law enforcement agencies. It is not always clear whether this stems from hacking or from collaboration between a few compromised officials and members of the cybercriminal underground.

In April 2023, Russia's Ministry of Internal Affairs told the press that it was conducting wide-reaching investigations of officials who are suspected of having sold to Ukrainian actors personal data belonging to security, law enforcement and judicial officials.[80]

It is not clear how many of these officials were targeted by call centres or hacking attacks on the basis of this data. However, Ukraine has publicly released personally identifiable information that it claims belongs to FSB officers.[81] Later in 2023, Russia's Ministry of Internal Affairs announced that it was laying off 5 000 officials in a restructuring to better enable the police to combat new law enforcement concerns, the most important being computer crimes.[82]

The scale of Ukrainian cybercrime has provided Moscow with additional justification to bolster its internal communications surveillance systems, under the auspices of detecting fraudulent phone calls. Rostelekom, the leading telecom provider in Russia, began to block IP addresses controlled by Russian hosting providers that offer digital anonymization services.[83] Roskomnadzor, the Russian Communications Monitoring and Censorship Directorate, received 1.54 billion rubles (US$17.6 million) to create a national monitoring system in 2022, but the system does not appear to have had much of an effect, given the continuing volume of scam calls emanating from Ukraine.[84]

Russia is moving to integrate the occupied regions of Ukraine into the coverage of Russian telecommunications providers and surveillance systems, namely SORM, a move that Russia claims is required to protect residents from call centre scams. The effect of this on the cybercriminal underground is not yet clear.[85]

A website advertises Russian databases for sale. Countless databases of personally identifiable information have been breached and resold on the cybercriminal underground.

The proliferation of these call centres and their broader criminal networks has not gone unnoticed by Ukrainian policymakers, however. In some cases, Ukrainian politicians have even been accused of involvement in these operations. The most prominent example of this is Nikola Tishchenko, a member of Ukraine's parliament, who fell under suspicion when audio clips featuring what appears to be his voice were shared on Telegram and with the Ukrainian press. In the audio clips, he claims to be able to protect call centre operations from legal authorities in exchange for monthly bribes.[86] He was placed under house arrest in the summer of 2024, where he remains as of writing while his business activities are investigated.[87] Tishchenko claims that he has actually been working to shut down such call centres and has avoided appearing in court as of writing, claiming to have health difficulties.[88]

The Verkhovna Rada, Ukraine's parliament, established a special commission to investigate the phenomenon and in July 2023 threatened to remove regional police management in Dnepropetrovsk if they continued to fail to address the issue.[89] Parliament pursued the investigation and in May 2024 passed legislation that created criminal penalties for such activity. However, it remains to be seen whether these laws will have an effect on the ground.[90] The call centres have continued to advertise on social media platforms such as TikTok and recruit new members, despite the new Ukrainian legislation.[91]

Russia's cyber front

One of the characteristics of military conflicts in the internet era is the increasing activity of 'hacktivist' groups that claim allegiance to one side in a conflict and perform cyberattacks against the digital infrastructure of the opposing armed forces and their allies. The relationships between such groups and the nation-states they support is often murky, providing degrees of plausible deniability for the government involved, and also potentially providing cover for more advanced nation-state activity,

At a press conference in March 2022, US corporations were warned to strengthen their defences against the threat of Kremlin-sponsored cyberattacks. *© Leigh Vogel/UPI/Bloomberg via Getty Images*

as data breached by such groups can be turned over to intelligence agencies before the hacks are uncovered and publicized.

Cybersecurity specialists for various governments have also been known to moonlight as cyber-criminals and hacktivists, making the delineations even more challenging. Hacktivists on both sides of the Russo-Ukrainian conflict recruit, organize, and claim responsibility for actions on messaging platforms such as Telegram and disclose their activity to the broader press.

Killnet is one of the most prominent hacktivist groups associated with Moscow. It formed shortly after Russia's full-scale invasion of Ukraine, and claimed to have approximately 4 500 members by April 2022.[92] It is difficult to determine the true relationships between Killnet and the Russian state or ransomware community, as the group has not shown high sophistication in its attacks. It has collaborated with other pro-Russian groups, such as UserSec, to perform DDoS attacks. The group currently has over 100 000 followers on Telegram. Much of its activity has involved nuisance-level DDoS attacks, marked by empty threats and claims that cannot be verified. Killnet has also collaborated with other online hacktivist groups, such as Anonymous Sudan, but the relationships are likely to be more of convenience than long-term ideological affinity.[93]

The Cyber Army of Russia is another group that has been active since the beginning of the war. It performs cyberattacks and hacks in support of Russian interests. Industry research published in April 2024 was able to connect the group to Sandworm, a hacking group that has been linked by security researchers and the US government to the Russian state, along with other online hacking personas, including Solntsepek and Xaknet.[94] The group is more sophisticated, and is suspected of hacking on behalf of Russian military intelligence and assisting in the targeting of Ukrainian military locations. The group may also be actively seeking collaborators inside Ukraine, where law enforcement claims to have arrested an IT specialist from eastern Ukraine who the group allegedly recruited over Telegram.[95]

Not surprisingly, following the much-publicized split between Conti ransomware group members at the beginning of the war, security researchers suspect that some of the Conti hackers in Russia are heavily involved in campaigns targeting Ukraine. Such actors specialize in gaining initial access to target

networks, using phishing emails and in some cases impersonating Ukraine's National Cyber Police.[96] Conti members are also likely to be behind the Akria ransomware group.[97]

Pro-Russian hacktivist groups such as Cyber Army of Russia Reborn have also threatened to target US and allied infrastructure, and have occasionally followed through on these threats, targeting industrial control systems in Europe and the US. These threats have led the US Critical Infrastructure Security Agency and European states to issue warnings and the US Department of the Treasury to sanction Russian hackers identified as responsible for performing or aiding such attacks.[98]

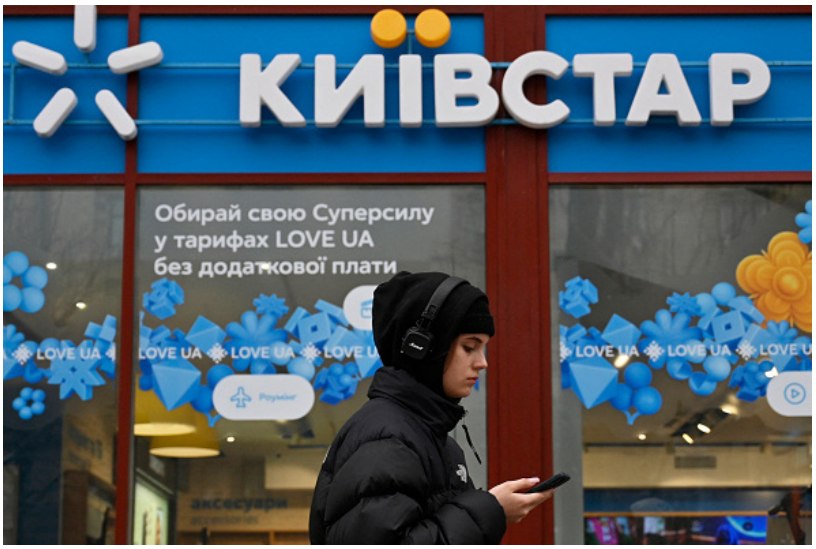
Ukraine's cyber front

Pro-Ukrainian hacktivists began to organize long before the Russian invasion, in response to some of the first aggressive cyberattacks against Ukraine, including the targeting of the country's power grid. The Cyber Alliance was formed in 2016, targeting Russian federal and local government sites. It successfully breached a major Russian broadcaster, document servers from Russia's Department of Defence, and the email of Russian presidential advisor Vladislav Surkov.[99] Since the outbreak of the war, the group has continued to carry out attacks against both Russian infrastructure and ransomware groups believed to be operating in Russia.[100]

Ukrainian hacktivists have had some success in hacking attacks that led to large breaches of personally identifiable information belonging to Russian citizens at the beginning of the war.[101] While Russian organizations increased their own cyber defence capabilities in response, large breaches of Russian personal information continue, including a massive breach of one of the country's largest banks, stealing data for 24 million citizens and 13 million legal entities.[102]

Ukraine's deputy minister of digital transformation, Mykhailo Fedorov, announced that an IT army was being formed shortly after the invasion to support Ukraine and that it would coordinate activities over Telegram.[103] This move led to the creation of the IT Army of Ukraine, which has nearly 150 000 subscribers to its Telegram channel as of writing, and most of the group's activities consist of internet scanning and DDoS attacks using specialized tools.

The group has organized DDoS attacks against a variety of targets in Russia, including ISPs, knocking some offline for extended periods, while it has also armed volunteers with DDoS attack tools free of



Ukraine's main phone operator, Kyivstar, denounced an act of war in December 2023, after a hacking attack led to widespread failure of its services. *© Sergei Chuzavkov/AFP via Getty Images*

charge.[104] In January 2024, Sberbank suffered its largest-ever DDoS attack, which lasted four days, when the IT Army of Ukraine targeted bank infrastructure.[105]

Ukrainian Blackjack is a group that the Ukrainian press has speculated is linked to Ukraine's security services, in particular the National Security Service.[106] It engages in more sophisticated attacks, including targeted espionage and destruction of data. One of the group's most recent attacks deployed malware targeting industrial control systems at a Russian company; it attempted to destroy sections of those systems.[107]

Ukrainian Blackjack is also developing a reputation for tit-for-tat retaliatory cyberattacks. When hacks against Ukraine's largest telecom provider, KyivStar, caused millions of euros worth of damage by destroying much of the company's core infrastructure and led to extended service interruptions for half of Ukraine's population in December 2023, the group responded with an attack in April 2024 by the aforementioned Blackjack group, which targeted Owencloud, a cloud provider in Russia. Blackjack claims to have destroyed 300 terabytes of data belonging to 10 000 firms, including companies in Russia's military-industrial complex.[108]

KibOrg is another such group that has targeted Russian companies, including Alfa Bank, Russia's largest private bank, with hacks leading to a data breach containing the institution's 40 million-strong client database.[109] As a result of pro-Ukrainian hacking attacks, the number of data breaches in Russia has increased: in 2023, over 220 million telephone numbers and 142 million emails were leaked as a result of these breaches against Russian companies, according to Solar, a leading Russian IT security firm, providing yet more targets for Ukrainian hackers and call centres.[110] InfoWatch, another Russian IT security firm, calculated that hacks against Russian organizations led to 1.12 billion accounts being breached in 2023, 60% more than in 2022.[111]

The war in Ukraine has vastly increased the number of individual targets for such hackers, as the lines between civilian and state have blurred. Any individual in Russia viewed as supportive of the invasion has now become a target for attacks by hacktivists, while Ukrainians are relentlessly targeted by Russian state-sponsored hacking groups.

Hacktivists had already been targeting the opposing side before the outbreak of the conflict. In 2016, Vladislav Surkov, Putin's special advisor, had his emails hacked and leaked by the Ukrainian outfit CyberHunta.[112] Kiber Soprotivlenie (Cyber Resistance) specializes in such attacks and has achieved various high-profile successes, including an email hack against Alexander Babakov, the deputy chairman of the Duma. Babakov is heavily involved in steering Russia's influence efforts in Africa and the Middle East. The hacked emails detailed the Kremlin's evaluation of Iran's experience with sanctions as precursor to tailoring Russia's own response to economic isolation, including how to offset the loss of traditional import sources.[113]

The same group breached an email account belonging to Semyon Bagdasarov, a high-ranking Duma member who has significant influence on foreign relations with Central Asia and the Middle East. Seven gigabytes worth of emails were leaked and published. These emails further detailed efforts by Russia to emulate Iran's sanctions avoidance policies and help Tehran further develop its energy export capabilities.[114]

Successful targeting of individuals continues, despite heightened security awareness within Russian government circles. Aleksei Zaklyazminsky, a personal advisor to former Russian president and current National Security Council Deputy Chairman Dmitry Medvedev, had his emails hacked in early 2024.

Initially, the data was transferred to Ukraine's intelligence services, before the hack was announced publicly months later.[115]

Russian hackers have performed their fair share of targeted intrusions against individuals, with one hacking group associated with Russian intelligence attempting to access hundreds of email accounts owned by various members of Ukraine's political leadership.[116] The most active Russian espionage group targeting Ukraine is tracked by the security community as Gamaredon, which continues to target a large volume military and political entities in Ukraine, as of writing.[117]

Ukrainian hacktivists have also taken to targeting ransomware outfits operating out of Russia. The Ukrainian Cyber Alliance successfully breached infrastructure belonging to Trigona ransomware in October 2023, leaking this group's internal documentation as well as data that it was holding ransom from victims around the world.[118]

As previously noted, the hacktivist groups maintain a reputation for exaggerating their own capabilities and making empty threats, so claims from these groups should always be taken with a pinch of salt until evidence is provided of their successful attacks. While there is good reason to suspect that these groups maintain ties to nation-states and overlap with government cyber specialists, there are also plenty of citizens who are interested in unilaterally aiding their country's war efforts. Some have therefore gained experience in cyber operations, especially since hacktivist groups openly share the tools that they use over the internet to increase their own attack power.

Wiper malware and the future of warfare

On the eve of Russia's invasion, Ukrainian infrastructure began to be targeted with a new strain of malware known as WhisperGate, which was designed to appear to be a ransomware variant. The attacks followed a standard ransomware model, with the victims' data appearing to be encrypted and a ransomware note displayed. Recovery teams soon discovered that the data itself was not encrypted, but destroyed by wiping the device's master boot record, making the files unrecoverable.[119]

The malware targeted IT contractors for the Ukrainian government, government agencies and nonprofits. The US Department of Justice indicted Amin Stigal, a 22-year-old Russian citizen, for his alleged role in the WhisperGate attacks in June 2024, accusing him of conspiring with Russia's main intelligence

In 2017, computer networks across Ukraine were infected with the Petya virus, which demanded ransom payment in cryptocurrency. *© Vincent Mundy/Bloomberg via Getty Images*

directorate (GRU) to target Ukrainian and NATO computer networks and offering a US$10 million reward for information on his location and activities.[120] Microsoft researchers were able to link the attacks to Russian military intelligence, noting that the attacks had relatively modest impact and low success rate, only affecting dozens of computer systems. The destructive attacks would serve as a foretaste of what Ukraine would experience in the coming months, however.[121]

Wiper malware packs the destructive punch of ransomware but does not wait for the victim to make a ransom payment, simply destroying any data it encounters as it spreads across networks. This particularly virulent strain of malware was rapidly deployed by both sides early in the conflict, with devastating results for both civilian and military infrastructure.

The Russo-Ukrainian war is not the first environment in which wiper malware has been deployed. Stuxnet, malware deployed by the US and Israel to target industrial control systems powering Iran's nuclear facilities, was first identified in 2010 and represents the most prominent early example of such technology being deployed.[122] Iran deployed Shamoon, another form of wiper malware, against Saudi Arabian oil facilities in 2012, destroying tens of thousands of hard drives before the incident could be contained. Wiper malware was also used in the NotPetya attacks, launched by a Russian state-sponsored actor in 2017 against a vast number of organizations in Ukraine before rapidly spreading around the world, and causing an estimated US$10 billion in damage.[123]

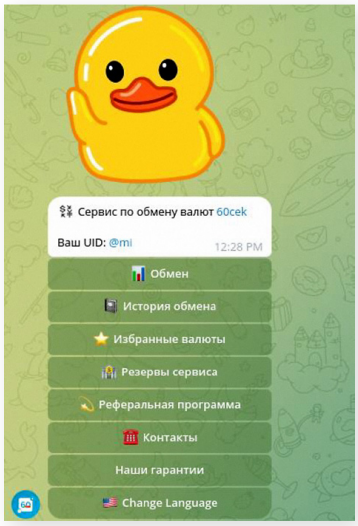
One of the most devastating initial wiper attacks was Russia's deployment of AcidRain, a data-destroying code that targeted Viasat satellite modems; it was used in March 2022 against the Ukrainian military to disrupt communications on the battlefield.[124] The attack put broad swathes of Ukraine's military communications offline. As was the case with Stuxnet, the malware spread out of the targeted country, eventually disrupting satellite communications in Germany.[125]

Ukraine eventually experienced a record for the number of wiper attacks in 2022, according to the cybersecurity firm ESET, which investigated several of the attacks, with one Russian state-sponsored hacking group alone carrying out 30 such cyberattacks in the first year of the war.[126] The wiper malware launched by Russian hackers has used a variety of different techniques to destroy data, from targeting database systems to overwriting files en masse with junk data. Research by one leading cybersecurity technology company found that wiper attacks increased by 54% in the 12 months following the start of the invasion.[127]

An AcidRain variant has been used again to target Ukrainian service providers, but Ukraine's government has stated that the effectiveness of cyberattacks targeting infrastructure declined significantly in 2023, a sign that the war is prompting long-term improvements in cyber defences.[128] Ukraine has also deployed its own wiper malware strains in cyberattacks, such as the aforementioned attacks by the Blackjack group in 2023 and 2024 that destroyed valuable data belonging to Russia's military industrial complex.

Crypto fuels sanctions evasion

American Express, Mastercard and Visa announced in early March 2022 that they were exiting the Russian market, shortly after the invasion of Ukraine. This and the substantial deepening of sanctions against Russia led to an increase in cryptocurrency transactions that year, building on regional and global growth in these highly unregulated markets over the previous decade.



A cryptocurrency exchange on Telegram.
Photo: Screenshot from Telegram

Estimates by Russia's central bank in a report shared with the press calculated that Russians performed 4.78 trillion rubles (US$52 billion) worth of transactions with cryptocurrencies in 2023. It also noted strong participation by the country's citizens in the cryptocurrency ecosystem, particularly through peer-to-peer and drop networks.[129]

Another study published in 2023 by a blockchain intelligence firm found that transactions on Russian-language cybercriminal sites accounted for US$1.5 billion worth of cryptocurrency transactions identified over the previous year, 80% of all transactions on darknet forums and marketplaces.[130] The US and Great Britain announced in March 2024 that they were investigating US$20 billion worth of sanctions violations in the form of cryptocurrency transactions performed on the cryptocurrency exchange Garantex using Tether, a stablecoin that is pegged to the US dollar. Garantex is a Moscow-based exchange that was first sanctioned in 2022.[131]

Despite the increased sanctions and surveillance, a large number of options remain in the region for cashing out illicit funds into cryptocurrency or using blockchains to shift money abroad. Telegram and online cryptocurrency exchanges allow a user to schedule a transfer from a bank account into cryptocurrency, or convert cryptocurrency into cash in multiple currencies that is instantly delivered by a courier service. Some exchanges on Telegram have performed over US$100 million worth of cryptocurrency transactions, according to a blockchain intelligence expert.[132]

Crypto: a money laundering dream

Cryptocurrencies have revolutionized cybercrime, both in terms of multiplying the avenues for making payments for illicit activity and with regard to laundering the proceeds of cybercrime. The anonymous nature of cryptocurrencies and easy accessibility of laundering services makes cashing out of hacked accounts simpler than other payment systems.

'Mixing' and 'tumbling' services are designed to make it even more difficult to trace the original source of a cryptocurrency transaction by moving the funds through a series of intermediary accounts, across various unregulated exchanges and between different cryptocurrencies. This frustrates attempts to track the source of transactions. These service providers charge a small commission for the operations.

The ease with which users can obfuscate ownership within the cryptocurrency realm has also lent itself to illicit mining efforts, and Russian-speaking cybercriminals have long pioneered the development of malware that can be deployed to steal computing power and mine cryptocurrency on compromised networks. Multiple botnets propagated over the past decade, such as Clipminer, are designed to gain initial access to a victim's infrastructure and then install cryptocurrency mining tools, generating revenue for the attackers.[133]

Cryptocurrency wallets have also become a prime target for cybercriminals. Malware is designed to steal users' wallet credentials, or to replace an intended recipient's address with that of an attacker during a cryptocurrency transaction.[134] ■

The war has also expanded the use of cryptocurrencies in Ukraine. Ukrainians who fled abroad have used cryptocurrencies to send money back to families who stayed behind after the invasion. Russia is also pioneering the development of blockchain technologies that can be used to perform international trade in the absence of access to international financial systems, such as the SWIFT inter-bank network, and amid efforts by hostile powers to seize the Kremlin's foreign currency reserves.[135]

Disputed zones such as Abkhazia and Transnistria have historically been pioneers in the legalization of crypto mining operations. Mining operations in Russia itself were estimated to earn around 11% of the US$1.5 billion generated every month by crypto mining around the world, according to the IMF.[136]

One blockchain intelligence expert noted that cryptocurrencies are now being widely used by individuals in President Putin's inner circle both to avoid sanctions, notably to facilitate arms imports, and for their own personal benefit, as their traditional methods for moving money offshore have been restricted by the sanctions.[137] Given the continued proliferation of sanctions targeting Russia's war efforts, it is very likely that the conflict will continue to expand the use of cryptocurrency in the broader region, driven by sanctioned governments, corrupt officials, ordinary citizens and cybercriminals alike.

Revival of Cold War-era corporate espionage?

In 1996, a series of hacks known as Moonlight Maze targeted a variety of US federal agencies' websites, exfiltrating confidential data related to submarine designs and other military technology. Twenty years later, researchers were able to piece together the original targeting in what they determined was the first case of state-on-state cyber espionage.[138] In the three decades since the original Moonlight Maze campaign, most of Russia's hacking efforts have been directed at nation-state objectives, not commercial industrial espionage.

In the aftermath of Russia's invasion of Ukraine, however, Putin has described continued dependence on Western technology as both 'humiliating' and 'dangerous'. He has called for full 'technological sovereignty' to be achieved in Russia, a goal that will be very difficult to achieve without industrial espionage, given the state of Russian industry on the eve of the war.[139]

Russia initially began to adopt import substitution policies in 2014 as the US and EU shifted to targeted sanctions in response to the annexation of Crimea and the support of militants in eastern Ukraine. However, this drive has achieved mixed results.[140] Over the past two years the Kremlin has unveiled a variety of strategies to promote the construction of advanced equipment needed for commodities extraction, electronics and microprocessors, as well as other manufacturing activity necessary for reducing reliance on the US, Europe and Japan.[141] Previous attempts undertaken under President Medvedev to develop an ecosystem for advanced technology along traditional lines, such as the Skolkovo Innovation Centre, were hobbled by corruption and inefficiencies.[142]

President Putin gave a speech in June 2022, shortly after the invasion of Ukraine, commemorating the 100th anniversary of the founding of the Sluzhba Vneshnei Razvedki (Foreign Intelligence Service). He lauded the 'incalculable role in the development of domestic technology and science' that Russia's military intelligence played during the Cold War, and also commemorated 'those who even today are performing unique operations, which are leading to the transfer of valuable information to the central government'.[143] This speech was interpreted by leading Russian media publications as the Kremlin giving a 'green light' to Russian hackers to increase their industrial espionage activities against Western companies.[144]

If relationships between Russia's cybercriminal underground and Russian security services have often been characterized by convenience and occasionally overlapping goals, the new realities of war and sanctions are very likely to lead to closer collaboration, according to interviews with experts on Russian state-sponsored hacking, as disclosed by a threat intelligence expert.[145] Ransomware groups have not generally appeared to pay much attention to the intellectual property that they have stolen before leaking the data on their websites, but the need for stolen technology to bolster the economies of Russia and its allies could very easily henceforth lead to such data being turned over to the Kremlin's security services before being put up for ransom.

Most Russian espionage since the outbreak of the war has so far remained focused on achieving short-term military objectives in Ukraine. There is no reason to believe that this will continue to be the case, however, according to an expert on nation-state hacking, speaking on condition of anonymity. 'All gloves are off' in terms of hacking targeting the West, this source noted.

The Kremlin is also cognizant of its increasing dependence on China since the outbreak of the war for many goods and technologies, and it does not want to become a vassal state with no industries beyond commodities exports. This compounds the need to develop its own industrial base.[146]

In the two years since the invasion, there are signs of increasingly brazen espionage against Western tech companies, including hacks of Microsoft's senior leadership in 2023 and Hewlett Packard by a Russian state-sponsored group known as Midnight Blizzard.[147] The Soviet Union devoted significant resources to industrial espionage in the last decades of the Cold War: many Eastern bloc diplomats worked as intelligence agents, mainly to facilitate technology theft, resulting in billions of dollars' worth of tech transfer to the Soviet defence industry and allowing the military-industrial base to compete with the US as the rest of the economy stagnated.[148] The Kremlin still possesses the expertise to perform such activity.

All of the conditions are in place for a revival of industrial espionage, and time will tell how aggressively the Kremlin decides to pursue the technological sovereignty it now covets and whether the hacks targeting US technology companies are the beginning of a broader trend.

RUSSIA'S CRACKDOWN ON INTERNET FREEDOM

The invasion of Ukraine has been accompanied by an unprecedented crackdown on internet freedom across Russia. The role of the internet in coordinating political protest came to the forefront during protests in 2011 and 2012 against President Putin's decision to seek a third term in office. The Kremlin's National Security Council began in 2016 to research the possibility of creating a domestic internet infrastructure that could function autonomously from the broader internet, in reaction to increasing concerns about the authorities' lack of control over cyberspace in the aftermath of their annexation of Crimea.[149]

Moscow's paranoia about digital security grew as millions of Russian citizens responded to the clamp-down on independent press in the weeks following the invasion of Ukraine by downloading VPNs to subvert the bans on websites imposed by the state.[150] Independent digital rights organizations claimed that as of late 2023, eight out of 15 popular VPN services had been blacklisted and did not work within the Russian Federation.[151]

VPN services on the Russian-language underground have responded to the latest anti-encryption measures, however, by quickly shifting their offerings to protocols, and maintaining servers in offshore jurisdictions outside Russia that offer better information privacy protection.[152] Many of these services also claim to avoid maintaining logs of user activity to frustrate user tracking in case their infrastructure is seized by law enforcement. Users on hacking and information security forums and Telegram channels are quick to distribute new information on how to potentially subvert new bans, and recommend new services to each other that offer secure VPNs that are not blocked by the Russian state.

Another key technological innovation enabling greater digital sovereignty is the development of a domestic security certificate ecosystem. Much of the internet's transport layer security (TLS) certificate-granting authority is located in the US, and these authorities exited the Russian and Belarusian markets in the weeks following the invasion of Ukraine.[153]

The Russian state had clearly been planning for this moment, as three Russian cryptographers published a paper through the Internet Engineering Task Force, the internet's main technical governing body, within weeks of the invasion, outlining cryptographic algorithms to underpin a new set of TLS certificates that would function in lieu of the traditional certificate-granting authorities, using the same x509 infrastructure.[154] Several of the cryptographers are employed by CryptoPro, a government

contractor that allegedly works closely with the FSB and develops cryptographic systems for the Russian security services.[155]

The Russian state instructed citizens to download the security certificate in order to execute various basic tasks, such as accessing online banking or municipal public services. Authorities also began to install the TLS certificate within leading Russian internet browsers, such as Yandex and Atom. Within a year and a half of the new TLS certificates, Sberbank estimated that approximately 30% of Russia's population had downloaded the certificates.[156] This TLS ecosystem opens up the possibility of eavesdropping and traffic interception, as the Russian state could, hypothetically, pressure the certificate issuers to snoop on user traffic and activities.[157]

The idea of a domestic TLS system was first explored by Kazakhstan in the 2010s, when the government attempted to convince citizens to download a custom TLS certificate system under the guise that it was needed to defend from cyberattacks.[158] International technology companies prevented the Kazakhstani TLS certificates from being compatible with their browsers, but Russia's TLS certificate system is a much better designed and sophisticated project.

This crackdown on civilian encryption will have wide-ranging consequences for ordinary Russians and the cybercriminal underground. Despite the chilling effect on civil society, this level of detection and censorship will not have the same level of impact on the cybercriminal underground, where knowledge of specialized VPN configurations to subvert censorship has existed for more than a decade. The VPN detection could also make it easier for Russia's security services to find less skilled would-be cybercriminals, however, who can potentially be pressured into pursuing the Kremlin's cyber objectives.

CONCLUSION

Organized crime has long thrived in stateless spaces and disputed legal territories, far from the prying eyes of international law enforcement. Cybercrime is not only confined to the digital arena, but relies on the bread and butter of traditional transnational organized criminal activity, such as smuggling networks, shell companies and money laundering schemes. While Russia and Ukraine are working to arrange a ceasefire, brokered by the US, the terms of this are far from certain.[159]

To make matters worse, migration out of Russia in the initial aftermath of the invasion has also led to cybercriminal activity expanding in Russia's near abroad. IT workers quickly banded together on digital platforms, such as Telegram, in the weeks following the invasion to coordinate plans to escape Russia.[160] Türkiye has hosted its own cybercriminal underground, which, although not as sophisticated as post-Soviet countries, contains a hacking scene that has focused on carding as well as nationalist hacktivism.

Cybercriminals began to set up shop in Türkiye as workers left Russia to work remotely in the aftermath of the invasion, with Russian cybercriminals quickly forming relationships with local carders. In some cases, the cybercriminals have begun to purchase property, often in Antalya, in order to obtain Turkish passports.

Turkish law enforcement has noted an increase in cybercrime, believed to stem from collaboration between Russian and Turkish cybercriminals, with Telegram emerging as a major method of education and collaboration.[161] Türkiye has a history of producing influential members of the global carding scene, including leading members of the DarkMarket forum, which was dismantled in 2008, so there is significant potential for Turkish cybercrime to further develop through increased collaboration.[162]

At the same time, the Kremlin has taken a number of measures to elevate IT workers to the status of a protected class and grant them as much state support as possible: the sector's workforce was shielded from draft orders, and the development of domestic software solutions to replace Western technology is now a strategic priority.[163] A large amount of state funding was made available in the form of grants, while mortgage incentives are offered to workers, and IT companies were granted a tax holiday through 2024.[164]

One expert on cyber warfare told the GI-TOC that as the Russia-Ukraine conflict increasingly degenerates into a war of attrition, cyberattacks remain a low-cost solution that can damage both military and civilian infrastructure without putting combatants in harm's way.[165]

Russian state-controlled oil giant Rosneft was among the victims of a global ransomware outbreak in 2017.
© Yuri Kadobnov/AFP via Getty Images

The amount of money generated by ransomware hit a new record in 2023, and the end of cooperation between Russian/Belarusian and international law enforcement stemming from frozen ties will only make it more difficult for perpetrators to be prosecuted. This will leave organizations in a permanent defensive posture. The arrest of members of the Revil ransomware gang by the FSB on the eve of the Ukraine invasion was interpreted by many as a signal from the Kremlin that its security services can turn ransomware attacks on and off at will.[166]

The shift toward remote work during the coronavirus pandemic is likely to have exacerbated the problem, as it has led to an expansion of many organizations' digital attack surfaces with more employees logged onto networks away from offices, and a rapid increase in ransomware attacks, particularly targeting VPNs and home routers. The shift towards cloud infrastructure, which can be challenging to monitor with traditional network technology tools, and towards the Internet of Things, will continue to expand the number of devices connected both to the internet and artificial intelligence, exacerbating internet security challenges.

The lack of extradition treaties between many post-Soviet states and the US has contributed to a sense of immunity among many members of the Russian-language underground, as long as they avoid travelling to countries that cooperate with US law enforcement. Sporadic cooperation between Russian and Belarusian law enforcement and their European and American counterparts has largely evaporated due to the unravelling of relations in recent years.

It is unlikely that cybercriminals will abstain from international travel and vacations forever, however. 'Sooner or later, these crooks are going to get tired of driving their Maseratis around Moscow,' noted one veteran security researcher. 'One of the main reasons a lot of them get into cybercrime is the access to money for ostentatious displays of wealth and international travel.'[167] The penchant among high-profile cybercriminals to vacation in warm-water locales that maintain extradition treaties has led

to multiple arrests in recent years, including that of Peter Yuryevich Levashov ('Severa'), the developer of the Kelihos botnet, who pleaded guilty in a US court in 2018.[168]

Ukrainian call centre fraud targeting Russians has been tolerated for a decade and it is doubtful that such activity will completely cease, despite Kyiv's recent legislation against it, at least as long as the conflict persists. This in turn will provide further grounds for the Kremlin to expand electronic surveillance. Meanwhile, Russian cybercriminals will increasingly concentrate on ransomware attacks and hacktivism in support of the Kremlin, while their Ukrainian counterparts will continue to focus their attention on hacking in defence of their homeland and operating the countless call centres that relentlessly target Russian citizens.

Ukrainian law enforcement began to increase cooperation with the rest of Europe and the US in the lead-up to Russia's invasion, and it now participates in regular conversations focusing on cybercrime, according to a senior European cybercrime investigator.[169]

Ukraine could also find that turning a blind eye to the proliferation of cybercrime targeting Russians proves only temporarily beneficial, and stores up significant problems beyond the current desperate fight for national survival. Such expertise will be difficult to dismantle in peacetime, particularly given the growing share of call centre fraud in the global cybercriminal economy.

The continued crackdown on civilian encryption technologies in Russia is having a chilling effect on civil society and will make it increasingly challenging for civilians to access the uncensored wider internet. The more tech-savvy cybercriminal underground will remain able to access VPNs, but could potentially run afoul of the Russian state's increasing surveillance at an ISP level. It is likely that their activities will continue to be tolerated, however, as long as they align with the Kremlin's strategic objectives and bring money into the country.

Wiper malware is also here to stay as a weapon in geopolitical conflict: it packs the punch of ransomware, but doesn't need to wait for a payment, and the effects are devastating for any organization, regardless of size. The war has also forced both sides to invest heavily in improving the security of as much public-facing internet infrastructure as possible, a formidable task as the number of exposed devices continues to increase daily.

Recommendations

Law enforcement must gain better visibility into blockchain activity to combat cybercrime. Communications from the Conti ransomware group revealed that they were seeking to develop their own blockchain technology.[170] As previously noted, blockchains have become key avenues that Russia has used to avoid sanctions and move money abroad.

Nonetheless, legal authorities can continue to target the infrastructure enabling cybercrime, including hosting providers that cater to the cybercriminal underworld operating in jurisdictions accessible by international law. Closer monitoring of cryptocurrency transactions, and associated exchanges, which have proliferated far from Russia and Ukraine but nonetheless cater to the underground, is an essential step in targeting the assets of cybercriminal entities.

Ukraine should work with allies to halt the call centre infrastructure that continues to target Russians: the longer such criminal networks persist, the more challenging it will be to disband them in a time of peace. Media reports have also noted that the call centre fraud is already targeting other countries.[171]

Experience from other conflict zones around the world demonstrates that illegal activities that are tolerated in wartime can prove to be very difficult to dismantle when the fighting ceases, as the illicit actors will often pivot into other areas of organized crime or sell their services to the highest bidders around the world.

Authorities should also closely monitor the development of Russia's internet surveillance system, as it will provide opportunities to co-opt the country's underground for state goals – and will most likely be replicated by other authoritarian states wishing to turn the tide against internet freedom.

Finally, the international community must also prepare for an influx of skilled hackers into the cyber-criminal underground once the conflict has ended, much as the 1990s transition to capitalism led many into carding and hacking. Despite efforts by international law enforcement, the underground continues to develop and to overcome temporary setbacks. The public and private sectors must prepare for the region's cybercrime to grow ever more sophisticated, feeding into continued global growth of this phenomenon.

NOTES

1 See the chapter Солдаты Криптографии in Вторжение: Краткая История Русских Хакеров, Moscow: Individuum Print, 2019, pp 2–3.

2 Daniil Turovskii, Вторжение: Краткая История Русских Хакеров, Moscow: Individuum Print, 2019, pp 45–50.

3 Vuzoteka, Вузы России со специальностью информационная безопасность, 10 March 2001, https://vuzoteka.ru/вузы/Информационная-безопасность-10-03-01.

4 Daniil Turovskii, Вторжение: Краткая История Русских Хакеров, Moscow: Individuum Print, 2019, p 159.

5 See, for example, Vadim Volkov, *Violent Entrepreneurs: The Use of Force in the Making of Russian Capitalism*, Ithaca, NY: Cornell University Press, 2002.

6 Andrei Soldatov, *The Red Web: The Struggle Between Russia's Digital Dictators and the New Online Revolutionaries*, New York: PublicAffairs, 2015, pp 115–120.

7 Leonid Losich, Белорусский кардер приговорен к 10 годам строгого режима с конфискацией, Gazetaby, 3 September 2009, https://gazetaby.com/post/belorusskij-karder-prigovoren-k-10-godam-strogogo-rezhima-s-konfiskaciej/23315/.

8 Как IT-индустрия развивает остальные отрасли экономики в 2022 году, Finance.ua, 12 December 2022, https://finance.ua/goodtoknow/jak-it-industrija-rozvyvae-inshi-galuzi-ekonomiky.

9 Sergei Krot, Доля IT в ВВП Беларуси снижается второй год подряд, Belsat, 23 September 2023, https://belsat.eu/ru/news/23-09-2023-dolya-it-v-vvp-belarusi-snizhaetsya-tretij-god-podryad.

10 Доля IT-отрасли в российском ВВП в прошлом году составила 1,96%, *Vedomosti*, 15 April 2024, https://www.vedomosti.ru/economics/news/2024/04/15/1031837-dolya-it-otrasli-rossiiskom-vvp.

11 Работа в IT самая прибыльная? Отрасли рынка труда Украины, где обещают высокий доход, RBC.ua, 15 March 2024, https://www.rbc.ua/ukr/news/robota-it-naypributkovisha-galuzi-rinku-pratsi-1710415297.html.

12 US Department of Justice, Ukrainian national who co-founded cybercrime marketplace sentenced to 18 years in prison, 12 December 2013, https://www.justice.gov/archives/opa/pr/ukrainian-national-who-co-founded-cybercrime-marketplace-sentenced-18-years-prison.

13 For a memoir describing this lifestyle, see Sergei Pavlovich, Как я украл миллион: Исповед раскаявшегося кардера, St Petersburg: Piter, 2014.

14 МВД: Российские хакеры - лучшие в мире, Lenta.ru, 11 April 2005, https://lenta.ru/news/2005/04/11/hackers/.

15 Sergei Pavlovich, Как я украл миллион: Исповед раскаявшегося кардера, St Petersburg: Piter, 2014, pp 207–208.

16 WebMoney – 25 years on! Changing the digital world for a quarter of a century, WebMoney, https://news.wmtransfer.com/en/blog/webmoney-25-years-on-changing-the-digital-world-for-a-quarter-of-a-century.

17 Sergei Pavlovich, Как я украл миллион: Исповед раскаявшегося кардера, St Petersburg: Piter, 2014, p 151.

18 US Department of Justice, Manhattan – U.S. Attorney announces charges against Liberty Reserve, one of world's largest digital currency companies, and seven of its principals and employees for allegedly running a $6 billion money laundering scheme, 28 May 2013, https://www.justice.gov/usao-sdny/pr/manhattan-us-attorney-announces-charges-against-liberty-reserve-one-world-s-largest.

19 Oleg Paramonov, Создаетля платёжной системы Liberty Reserve посадили на 20 лет, *Hacker*, 10 May 2016, https://xakep.ru/2016/05/10/arthur-budovsky/.

20 US Department of Justice, Cybercriminal marketplace disrupted in international cyber operation, 5 April 2023, https://www.justice.gov/opa/pr/criminal-marketplace-disrupted-international-cyber-operation.

21 Interview with a cybercrime expert and law enforcement veteran, 25 April 2024.

22 Interview with a cybercrime expert, 29 April 2024.

23 Joe Tidy, 74% of ransomware revenue goes to Russia-linked hackers, BBC, 14 February 2022, https://www.bbc.com/news/technology-60378009.

24 Chainalysis, Ransomware payments exceed $1 billion in 2023, hitting record high after 2022 decline, 7 February 2024, https://www.chainalysis.com/blog/ransomware-2024/.
25 OSINTer, Popular Russian hacking forum XSS bans all ransomware topics, 13 May 2021, https://osinter.dk/article/476d69816667165d159442baf3e16723.
26 Interview with a cybercrime expert, 24 April 2024.
27 Interview with a cybercrime intelligence analyst and expert, 12 April 2024.
28 Intel 471, Here's who is powering the bulletproof hosting market, 3 March 2021, https://intel471.com/blog/top-bulletproof-hosting-providers-yalishanda-ccweb-brazzzers-2021; interview with an industry source, 17 April 2024.
29 Interview with a cybercrime expert, 29 April 2024.
30 Border Gateway Protocol data examined by the author, and interview with a cybercrime expert, 30 April 2024.
31 Interview with a European federal law enforcement expert on cybercriminal hosting, 30 April 2024.
32 See Fast Flux Hosting and DNS, ICANN SSAC, https://ccnso.icann.org/files/atlarge/ssac-fast-flux-hosting.
33 Dmitro Demchenko, СБУ разоблачила одесского хакера. Он причастен к взлому NASDAQ, атакам на инфраструктуру Украины и нанес ущерб на $300 млн, Ain.ua, 16 July 2019, https://ain.ua/ru/2019/07/16/sbu-razoblachenie-xakera/.
34 US Department of Justice, Five indicted in New Jersey for largest known data breach conspiracy, 25 July 2013, https://www.justice.gov/usao-nj/pr/five-indicted-new-jersey-largest-known-data-breach-conspiracy.
35 Evgen Shishatskii, История на $305 млн. СБУ задержала «повелителя даркнета»? Детали, Liga.net, 16 July 2019, https://tech.liga.net/technology/article/istoriya-na-305-mln-sbu-zaderjala-ochen-krupnogo-hakera-detali.
36 See Mykhaylo Sergiyovich Rytikov, United States Secret Service: Most wanted, https://www.secretservice.gov/investigations/mostwanted/rytikov. For Rytikov's claims in court, see Украинский хакер выиграл суд против СБУ о защите чести и достоинства, Dev.ua, 13 October 2021, https://dev.ua/ru/news/rytikov,.
37 Interview with an industry source, 18 April 2024.
38 See ThreatFox database, https://threatfox.abuse.ch/browse/tag/AS-ALVIVA.
39 A web banner is an advertisement displayed on the world wide web, delivered by an ad server. These banners are designed to direct traffic to a website via links to the advertiser's infrastructure.
40 Fyodor Yarochkin and Vladimir Kropotov, Lurk: Retracing the group's five-year campaign, Trend Micro, 7 February 2017, https://www.trendmicro.com/en_us/research/17/b/lurk-retracing-five-year-campaign.html.
41 See Chapter 2 in Brian Krebs, *Spam Nation: The Inside Story of Organized Cybercrime–from Global Epidemic to Your Front Door*, New York: Sourcebooks, 2014.
42 Interview with a long-time expert on Russian-language cybercrime, 29 April 2024.
43 Daniil Turovskii, Вторжение Краткая История Русских Хакеров, Moscow: Individuum Print, 2019.
44 Фигурирующий в деле о госизмене сотрудник ФСБ в прошлом был хакером, RBC, 27 January 2017, https://www.rbc.ru/society/27/01/2017/588b07ba9a79472f625421ea. Dokuchaev's role as an FSB officer is confirmed in a 2017 indictment. See US Department of Justice, U.S. charges Russian FSB officers and their criminal conspirators for hacking Yahoo and millions of email accounts, 15 March 2017, https://www.justice.gov/archives/opa/pr/us-charges-russian-fsb-officers-and-their-criminal-conspirators-hacking-yahoo-and-millions.
45 Осужденный за госизмену экс-сотрудник ФСБ Докучаев освобожден по УДО, Interfax, 13 May 2021, https://www.interfax.ru/russia/765872.
46 Anton Cherepanov and Robert Lipovsky, VB2016 paper: BlackEnergy – what we really know about the notorious cyber attacks, *Virus Bulletin*, October 2016, https://www.virusbulletin.com/virusbulletin/2017/07/vb2016-paper-blackenergy-what-we-really-know-about-notorious-cyber-attacks/.
47 GameOver ZeuS: Backgrounds on the badguys and the backends, Black Hat, 2015, https://www.blackhat.com/docs/us-15/materials/us-15-Peterson-GameOver-Zeus-Badguys-And-Backends-wp.pdf.
48 US Department of Justice, U.S. charges Russian FSB officers and their criminal conspirators for hacking Yahoo and millions of email accounts, 15 March 2017, https://ru.usembassy.gov/u-s-charges-russian-fsb-officers-criminal-conspirators-hacking/.
49 US Department of Justice, International hacker-for-hire who conspired with and aided Russian FSB officers sentenced to 60 months in prison, 29 May 2018, https://www.justice.gov/opa/pr/international-hacker-hire-who-conspired-and-aided-russian-fsb-officers-sentenced-60-months.
50 Dina Temple-Raston, A Q&A with Wazawaka: The FBI's cyber most wanted says new designation won't affect his work, *The Record*, 30 May 2023, https://therecord.media/wazawaka-cyber-most-wanted-interview-click-here.
51 US Department of Justice, Russian national charged with ransomware attacks against critical infrastructure, 16 May 2023, https://www.justice.gov/opa/pr/russian-national-charged-ransomware-attacks-against-critical-infrastructure.
52 Daryna Antoniuk, Ransomware suspect Wazawaka reportedly arrested by Russia, *The Record*, 2 December 2024, https://therecord.media/wazawaka-mikhail-matveev-reportedly-arrested-russia.

53 US Department of the Treasury, Treasury sanctions Evil Corp, the Russia-based cybercriminal group behind Dridex malware, 5 December 2019, https://home.treasury.gov/news/press-releases/sm845.

54 UK National Crime Agency, Evil Corp: Behind the scenes, October 2024, https://www.nationalcrimeagency.gov.uk/who-we-are/publications/732-evil-corp-behind-the-screens/file.

55 US Department of Justice, Russian national indicted for series of ransomware attacks, 1 October 2024, https://www.justice.gov/opa/pr/russian-national-indicted-series-ransomware-attacks.

56 US Department of Justice, Russian national charged with decade-long series of hacking and bank fraud offenses resulting in tens of millions in losses and second Russian national charged with involvement in deployment of 'Bugat' malware, 5 December 2019, https://www.justice.gov/opa/pr/russian-national-charged-decade-long-series-hacking-and-bank-fraud-offenses-resulting-tens.

57 In lavish wedding photos, clues to an alleged Russian cyberthief's FSB family ties, RFE/RL, 11 December 2019, https://www.rferl.org/a/in-lavish-wedding-photos-clues-to-an-alleged-russian-cyberthief-fsb-family-ties/30320440.html.

58 US Department of the Treasury, Treasury sanctions members of the Russia-based cybercriminal group Evil Corp in tri-lateral action with the United Kingdom and Australia, 1 October 2024, https://home.treasury.gov/news/press-releases/jy2623.

59 Conti ransomware group announces support for Russian invasion of Ukraine, threatens retaliation, SC Media, 25 February 2022, https://www.scmagazine.com/news/conti-ransomware-group-announces-support-for-russian-invasion-of-ukraine-threatens-retaliation.

60 Interview with an expert on state-sponsored hacking, 29 April 2024.

61 Discussion on a carding forum, 2022.

62 Mariya Nefyedova, Внутренние чаты хак-группы Conti слили в открытый доступ, *Hacker*, 1 March 2022, https://xakep.ru/2022/03/01/conti-chats-leak/.

63 Interview with a security researcher, 29 March 2024.

64 Interview with a Russian-speaking hacker, 20 July 2024.

65 Interview with a Russian-speaking hacker, 10 August 2024.

66 Interview with a cybersecurity researcher, 29 April 2024.

67 Mark Galeotti, Time of troubles: The Russian underworld since the Ukraine invasion, GI-TOC, 4 December 2023, https://globalinitiative.net/analysis/the-russian-underworld-since-the-ukraine-invasion/.

68 В России и аннексированном Крыму за пять дней не меньше 28, *Meduza*, 2 August 2023, https://meduza.io/feature/2023/08/02/v-rossii-i-anneksirovannom-krymu-za-pyat-dney-ne-menshe-28-raz-pytalis-podzhech-voenkomaty.

69 «За обман русских мне ничего не будет» Телефонные мошенники атакуют россиян с Украины. Как работают их кол-центры?, Lenta.ru, 11 August 2023, https://lenta.ru/articles/2023/08/11/call/.

70 Aleksei Sakhnin, Как работают мошеннические колл-центры, потрошащие счета наивных москвичей, 6 April 2023, *Moskvich Mag*, https://moskvichmag.ru/lyudi/kak-rabotayut-moshennicheskie-koll-tsentry-potroshashhie-scheta-naivnyh-moskvichej/. For attacks on journalists, see Вырывали телефон и разбили нос: В столичном БЦ «Алмаз» работники мошеннического колл-центра избили журналистов, Stop Korruption Ukraina, 8 March 2024, https://www.stopcor.org/section-uanews/news-zuhvalij-napad-na-zhurnalistiv-u-stolichnomu-bts-almaz-pratsivniki-shahrajskogo-kol-tsentru-pobili-medijnikiv-08-03-2024.html.

71 Ibid.

72 Тысячи «сотрудников», взятки, крипта и пытки: как устроены мошеннические колл-центры в Украине, Informator, 26 July 2023, https://informator.ua/ru/tysyachi-sotrudnikov-vzyatki-kripta-i-pytki-kak-ustroeny-moshennicheskie-koll-centry-v-ukraine. For the estimate of 120 000, see В Днепре при участии нардепа Тищенко устроили облаву на колл-центры, Dnepr.Express, 20 June 2024, https://dnepr.express/ru/post/v-dnepre-pri-uchastii-nardepa-tishenko-ustroili-oblavu-na-koll-centry.

73 В Сбербанке сообщили о раскрытом в Бердянске колл-центре мошенников, *Vedomosti*, 3 June 2022, https://www.vedomosti.ru/society/news/2022/06/03/925101-sberbanke-berdyanske-koll-tsentre; Сбербанк рассказал о раскрытой в Бердянске сети колл-центров мошенников, RIA Novosti, 3 June 2022, https://ria.ru/20220603/moshenniki-1793003272.html.

74 Как работают мошеннические колл-центры, потрошащие счета наивных москвичей, *Moskovich Magazin*, 6 April 2023, https://moskvichmag.ru/lyudi/kak-rabotayut-moshennicheskie-koll-tsentry-potroshashhie-scheta-naivnyh-moskvichej/.

75 ФСБ пресекла деятельность проукраинских мошеннических call-центров в Москве, *Izvestiya*, 26 April 2023, https://iz.ru/1504430/2023-04-26/fsb-presekla-deiatelnost-proukrainskikh-moshennicheskikh-koll-tcentrov-v-moskve.

76 В Москве сожгли BMW сотрудника Генштаба. Родственники подозреваемой говорят о гипнозе, Gazeta.ru, 28 August 2022, https://www.gazeta.ru/social/2022/08/28/15342554.shtml; Москвичку, которая подожгла BMW сотрудника Генштаба, могли обмануть, Radio Svoboda, 28 August 2022, https://www.svoboda.org/a/moskvichku-kotoraya-podozhgla-bmw-sotrudnika-genshtaba-mogli-obmanutj/32007877.html (first reported on Telegram: https://t.me/bazabazon/12957).

77 Миронов предложил Минобороны рассматривать украинские колл-центры как военные объекты, *Vedomosti*, 7 August 2023, https://www.vedomosti.ru/politics/articles/2023/08/07/988970-mironov-predlozhil-rassmatrivat-ukrainskie-koll-tsentri.

78 Ibid.

79 Телефонное мошенничество в России, Часть 1, Sberbank, https://www.sberbank.ru/ru/person/kibrary/investigations/berdyansk-glava-2.

80 Массовые проверки проходят в УВД по ЦАО Москвы из-за утечки данных российских силовиков, TASS, 19 April 2023, https://tass.ru/proisshestviya/17559435.

81 Ukraine intelligence publishes names of 620 alleged Russian agents, Reuters, 28 March 2022, https://www.reuters.com/world/europe/ukraine-intelligence-publishes-names-620-alleged-russian-agents-2022-03-28/.

82 Глава МВД РФ заявил об увольнении из ведомства 5 тыс. сотрудников в июле, Interfax, 10 August 2023, https://www.interfax.ru/russia/915654.

83 ФСБ обязала «Ростелеком» зачистить IP-телефонию. От мошенников, CNews, 15 March 2024, https://www.cnews.ru/news/top/2024-03-15_fsb_obyazala_rostelekom.

84 Власти потратят 1,88 миллиарда на ИТ-системы контроля телефонных звонков, CNews, 31 August 2022, https://www.cnews.ru/news/top/2022-08-31_vlasti_potratyat_188_milliarda.

85 Ловушка в телефоне: зачем РФ переводит оккупированный Донбасс на российские номера, Radio Svoboda, 10 October 2023, https://www.radiosvoboda.org/a/donbas-mobilnyy-zvyazok-okupatsiya/32538992.html.

86 «Слуга» Николай Тищенко принялся бороться с call-центрами – СМИ, *Fokus*, 24 August 2023, https://focus.ua/ukraine/587861-sluga-mikola-tishchenko-zahodivsya-borotisya-z-call-centrami-zmi.

87 Николай Тищенко пытается избежать продолжения домашнего ареста: суд еще раз перенесли, Stop Korruption Ukraina, 14 November 2024, https://www.stopcor.org/section-uanews/news-mikola-tischenko-namagaetsya-uniknuti-prodovzhennya-domashnogo-areshtu-sud-vkotre-perenesli-14-11-2024.html.

88 Несмотря на состояние здоровья и арест: как Николай Тищенко оказался на заседании Верховной Рады, *Fokus*, 8 January 2025, https://focus.ua/eksklyuzivy/687448-nikolay-tishchenko-pod-arestom-pochemu-deputat-poyavilsya-v-rade-novosti-ukrainy.

89 Полиции, СБУ и прокуратуре дали месяц на борьбу с кол-центрами в Днепре – выездная ВСК Верховной Рады, Informator, 25 July 2023, https://informator.ua/ru/policii-sbu-i-prokurature-dali-mesyac-na-borbu-s-koll-centrami-v-dnepre-vyezd-vsk-verhovnoy-rady.

90 Liudmila Prisyazhnaya, Рада поддержала в первом чтении законопроект о борьбе с незаконными колл-центрами, Ligazakon, 22 May 2024, https://biz.ligazakon.net/ru/news/227904_rada-podderzhala-v-pervom-chtenii-zakonoproekt-o-borbe-s-nezakonnymi-koll-tsentrami.

91 Darya Yakimets, Депутаты голосуют, а «офисы» – работают: в Киеве мошеннические колл-центры продолжают вербовать работников, Stop Korruption Ukraina, 22 May 2024, https://www.stopcor.org/section-suspilstvo/news-deputati-golosuyut-a-ofisi-pratsyuyut-u-kievi-shahrajski-kol-tsentri-prodovzhuyut-verbuvati-pratsivnikiv-22-05-2024.html.

92 Artur Galeev, «Не надо было угрожать моей стране» Хакеры Killnet защищают Россию, сражаясь с Anonymous и НАТО. Кто за ними стоит?, Lenta, 15 April 2022, https://lenta.ru/articles/2022/04/15/killnet/.

93 Simon Hendery, Anonymous Sudan DDoS strikes dominate attacks by KillNet collective, SCWorld, 20 July 2024, https://www.scworld.com/news/anonymous-sudan-ddos-strikes-dominate-attacks-by-killnet-collective.

94 AJ Vicens and Christian Vasquez, Mandiant: Notorious Russian hacking unit linked to breach of Texas water facility, CyberScoop, 17 April 2024, https://cyberscoop.com/sandworm-apt44-texas-water-facility/. The US Department of Justice has linked the hackers to the Russian state in an indictment from 15 October 2020 – see *United States of America v. Yuriy Sergeyevich Andrienko et al*, United States District Court Western District of Pennsylvania, 15 October 2020, https://www.justice.gov/archives/opa/press-release/file/1328521/d.

95 Daryna Antoniuk, Ukraine's security service detains member of Russian 'Cyber Army', *The Record*, 26 January 2024, https://therecord.media/ukraine-detains-member-of-russia-cyber-army.

96 Pierre-Marc Bureau, Initial access broker repurposing techniques in targeted attacks against Ukraine, 7 September 2022, Threat Analysis Group, https://blog.google/threat-analysis-group/initial-access-broker-repurposing-techniques-in-targeted-attacks-against-ukraine/.

97 Health Sector CyberSecurity Coordination Center, HC3 analyst note, 7 February 2024, https://www.hhs.gov/sites/default/files/akira-randsomware-analyst-note-feb2024.pdf.

98 US Department of the Treasury, Treasury sanctions leader and primary member of the Cyber Army of Russia Reborn, 19 July 2024, https://home.treasury.gov/news/press-releases/jy2473.

99 Об украинских хактивистах, кибервойне и уязвимостях в госсекторе. Интервью с членом Ukrainian Cyber Alliance Андреем Барановичем, Dua.ua, 4 February 2021, https://dou.ua/lenta/interviews/story-of-ukrainian-cyber-alliance/.

100 Natalya Khandusenko, Хактивисты «Украинского киберальянса» уничтожили серверы российских киберпреступников, Dev.ua, 18 October 2023, https://dev.ua/ru/news/khaktyvisty-ukrainskoho-kiberaliansu-znyshchyly-servery-rosiiskykh-kiberzlochyntsiv-1697641918.

101 Опасность интернет-магазинов и маркетплейсов: украинские хактивисты крадут данные россиян, Dzen.ru, https://dzen.ru/a/ZapH1k2ZVEKgiFiT.

102 Anastasia Zharikova, Украинские хакеры слили в сеть данные всех клиентов российского «Альфа-Банка», Ekonomichna Pravda, 8 January 2024, https://www.epravda.com.ua/rus/news/2024/01/8/708515/.

103 Elena Roschina, Создаем IT-армию – Федоров, Ukrainska Pravda, 26 February 2022, https://www.pravda.com.ua/rus/news/2022/02/26/7326225/.

104 IT-армия Украины запустила приложение для ddos-атак на российские ресурсы, рассчитанное на разный уровень знаний в ИТ, Dev.ua, 6 December 2023, https://dev.ua/ru/news/it-army-kit-1701863020.

105 Natalya Khandusenko, Сбербанк россии подвергся самым мощным DDoS-атакам, Dev.ua, 15 February 2024, https://dev.ua/ru/news/sbierbank-rf-ddos-ataka-it-army-of-ukraine-1708000535.

106 See, for example, Группа украинских хакеров взломала серверы московского интернет-провайдера: готовятся к мести за атаку на «Киевстар», Delo.ua, 9 January 2024, https://delo.ua/ru/business/gruppa-ukrainskix-xakerov-vzlomala-servery-moskovskogo-internet-provaidera-gotovyatsya-k-mesti-za-ataku-na-kievstar-427978/.

107 Pierluigi Paganini, Ukrainian Blackjack Group used ICS malware Fuxnet against Russian targets, Security Affairs, 15 April 2024, https://securityaffairs.com/161865/hacking/blackjack-ics-malware-fuxnet.html.

108 Russian hackers were inside Ukraine telecoms giant for months, Reuters, 5 January 2024, https://www.reuters.com/world/europe/russian-hackers-were-inside-ukraine-telecoms-giant-months-cyber-spy-chief-2024-01-04/; Украинские хакеры стёрли более 300 террабайт данных в российском дата-центре, Reform.news, 8 April 2024, https://reform.news/ukrainskie-hakery-stjorli-bolee-300-terrabajt-dannyh-v-rossijskom-data-centre.

109 Хакеры слили в сеть полную базу российского Альфа-Банка – это данные почти 40 млн клиентов, Obozrevatel, 8 January 2024, https://www.obozrevatel.com/ekonomika-glavnaya/economy/hakeryi-slili-v-set-polnuyu-bazu-rossijskogo-alfa-banka-eto-dannyie-pochti-40-mln-klientov.htm.

110 ГК «Солар»: число утекших телефонных номеров в 2023 году в 1,5 раза превысило численность населения РФ, Solar, 15 December 2023, https://rt-solar.ru/events/news/3932/.

111 Аналитики оценили рост утечек персональных данных в России, RBC, 11 March 2024, https://www.rbc.ru/society/11/03/2024/65ec41e89a7947dc41bd43f9.

112 Alya Shandra and Robert Seely, The Surkov leaks: The inner workings of Russia's hybrid war in Ukraine, RUSI, 16 July 2019, https://rusi.org/explore-our-research/publications/occasional-papers/surkov-leaks-inner-workings-russias-hybrid-war-ukraine.

113 InformNapalm: Взлом почты зампредседателя Госдумы РФ Александра Бабакова – формирование «пятых колонн» в мире, обход санкций и коррупционные схемы, Investigator, 21 August 2023, https://investigator.org.ua/news-2/257824/.

114 BagdasarovLeaks: Взлом экс-депутата Госдумы РФ Семена Багдасарова. Иранский гамбит, InformNapalm, 5 April 2023, https://informnapalm.org/52566-bagdasarovleaks-vzlom-semen-bagdasarov/.

115 Maryana Polishuk, Украинские хакеры опубликовали письма из электронной почты помощника Дмитрия Медведева, Korotko Pro, 27 June 2024, https://kp.ua/politics/a692568-ukrainskie-khakery-opublikovali-pisma-po-pochte-pomoshchnika-dmitrija-medvedeva.

116 Ravie Lakshmanan, APT28 targets Ukrainian government entities with fake 'Windows Update' emails, The Hacker News, 1 May 2023, https://thehackernews.com/2023/05/apt28-targets-ukrainian-government.html.

117 Zoltan Rusnak, Cyberespionage the Gamaredon way: Analysis of toolset used to spy on Ukraine in 2022 and 2023, WeLiveSecurity, 26 September 2024, https://www.welivesecurity.com/en/eset-research/cyberespionage-gamaredon-way-analysis-toolset-used-spy-ukraine-2022-2023/.

118 Ionut Ilascu, Ukrainian activists hack Trigona ransomware gang, wipe servers, Bleeping Computer, 18 October 2023, https://www.bleepingcomputer.com/news/security/ukrainian-activists-hack-trigona-ransomware-gang-wipe-servers/.

119 Pedro Tavares, WhisperGate: A destructive malware to destroy Ukraine computer systems, InfoSec Institute, 25 May 2022, https://www.infosecinstitute.com/resources/malware-analysis/whispergate-a-destructive-malware-to-destroy-ukraine-computer-systems/.

120 US Department of Justice, Russian national charged for conspiring with Russian military intelligence to destroy Ukrainian government computer systems and data, 26 June 2024, https://www.justice.gov/opa/pr/russian-national-charged-conspiring-russia-military-intelligence-destroy-ukrainian.

121 Microsoft: Russia sent its B team to wipe Ukrainian hard drives, The Register, 16 June 2023, https://www.theregister.com/2023/06/16/microsoft_cadet_blizzard_threat/.

122 See Kim Zetter, *Countdown to Zero Day: Stuxnet and the launch of the world's first digital weapon*, New York: Crown Publishers, 2014.

123 A year of wipers: How the Kremlin-backed Sandworm has attacked Ukraine during the war, *The Record*, 1 March 2023, https://therecord.media/a-year-of-wipers-how-the-kremlin-backed-sandworm-has-attacked-ukraine-during-the-war.

124 Jai Vaijayan, Russian APT releases more deadly variant of AcidRain wiper malware, Dark Reading, 22 March 2024, https://www.darkreading.com/cyberattacks-data-breaches/russian-apt-releases-more-deadly-variant-of-acidrain-wiper-malware.

125 Jonathan Reed, AcidRain malware shuts down thousands of modems in Ukraine, Security Intelligence, 18 May 2022, https://securityintelligence.com/news/acidrain-malware-modems-ukraine-germany/.

126 Ukraine suffered more data-wiping malware last year than anywhere, ever, *Wired*, 22 February 2023, https://www.wired.com/story/ukraine-russia-wiper-malware/; Cybersecurity & Infrastructure Security Agency, Update: Destructive malware targeting organizations in Ukraine, 28 April 2022, https://www.cisa.gov/news-events/cybersecurity-advisories/aa22-057a.

127 Jai Vijayan, Wiper malware surges ahead, spiking 53% in 3 months, Dark Reading, 23 February 2023, https://www.darkreading.com/cyberattacks-data-breaches/wiper-malware-surges-ahead-spiking-53-in-3-months.

128 Kevin Poireault, Cyber-attacks on Ukraine surge 123%, but success rates plummet, *InfoSecurity Magazine*, 27 September 2023, https://www.infosecurity-magazine.com/news/cyberattacks-ukraine-surge-success/.

129 Банк России оценил объем операций россиян с криптовалютой, RBC, 1 April 2024, https://www.rbc.ru/crypto/news/660a69279a79472fdf85f418.

130 David Hollingworth, Russian sites make up 80% of all darknet transactions, CyberDaily, 10 July 2023, https://www.cyberdaily.au/security/9290-russian-sites-make-up-80-per-cent-of-all-darknet-transactions.

131 Oleg Davygora, США и Великобритания расследуют переводы криптовалют на российскую биржу, Unian, 28 March 2024, https://www.unian.net/world/ssha-i-velikobritaniya-rassleduyut-perevody-kriptovalyut-na-rossiyskuyu-birzhu-12587253.html.

132 Interview with a blockchain intelligence expert, 30 April 2024.

133 Symantec, Clipminer botnet makes operators at least $1.7 million, Symantec Threat Intelligence, 2 June 2022, https://symantec-enterprise-blogs.security.com/blogs/threat-intelligence/clipminer-bitcoin-mining-hijacking.

134 5 crypto-stealing malware threats: How to stay safe and aware, HackerNoon, 18 August 2023, https://hackernoon.com/5-crypto-stealing-malware-threats-how-to-stay-safe-and-aware.

135 Путин подписал закон о использовании ЦФА в международных расчетах, RBC, 11 March 2024, https://www.rbc.ru/crypto/news/65ef111f9a794772819a1e83.

136 МВФ назвал способ ухода от санкций с помощью майнинга криптовалют, RBC, 20 April 2022, https://www.rbc.ru/crypto/news/625fd4f69a79470495afe85c.

137 Interview with a blockchain intelligence expert, 20 July 2024.

138 Juan Andres Guerrero-Saade et al, Penquin's Moonlit Maze, Kaspersky Lab, 3 April 2017, available at: https://ridt.co/d/jags-moore-raiu-rid.pdf.

139 Импортозамещение и технологический суверенитет. Владимир Путин на Госсовете обсудил пакет мер поддержки промышленности России, *Rossiyskaya Gazeta*, 4 April 2023, https://rg.ru/2023/04/04/reg-cfo/razvivat-s-umom.html.

140 Heli Simola, Russia is struggling to find new sources of imports, *Bank of Finland Bulletin*, 26 August 2022, https://www.bofbulletin.fi/en/blogs/2022/russia-is-struggling-to-find-new-sources-of-imports.

141 Русские чипы и материнские платы: импортозамещение электроники набирает обороты, Dzen, 22 December 2023, https://dzen.ru/a/ZYXK9UJmzHvbI1bM.

142 Masha Borak, How Russia killed its tech industry, *MIT Technology Review*, 4 April 2023, https://www.technologyreview.com/2023/04/04/1070352/ukraine-war-russia-tech-industry-yandex-skolkovo/.

143 Владимир Путин поздравил сотрудников и ветеранов СВР со столетием нелегальной разведки, Kremlin.ru, 30 June 2022, http://kremlin.ru/events/president/news/68790.

144 Путин напомнил разведчикам о важности промышленного шпионажа, Kommersant, 30 June 2022, https://www.kommersant.ru/doc/5436825.

145 Interview with a threat intelligence expert focused on Russian state-sponsored attacks, 11 April 2024.

146 Interview with an expert on state-sponsored hacking and cyberwarfare, 29 April 2024.

147 Lorenzo Franceschi-Bicchierai, Russian spies keep hacking into Microsoft in 'ongoing attack,' company says, TechCrunch, 8 March 2024, https://techcrunch.com/2024/03/08/microsoft-ongoing-cyberattack-russia-apt-29/; US Cybersecurity and Infrastructure Security Agency, CISA directs federal agencies to immediately mitigate significant risk from Russian state-sponsored cyber threat, 11 April 2024, https://www.cisa.gov/news-events/news/cisa-directs-federal-agencies-immediately-mitigate-significant-risk-russian-state-sponsored-cyber.

148 US Central Intelligence Agency, How Soviets steal U.S. high-tech secrets, *U.S. News and World Report*, 12 August 1985, https://www.cia.gov/readingroom/docs/CIA-RDP90-00965R000201730002-0.pdf.

149 Клименко допустил отключение России от 'мирого интернета', TV Rain, 29 December 2016, https://tvrain.tv/news/klimenko-424551/.

150 The Global Security Market, Secure VPN usage sees major uptick in Russia, 20 August 2022, https://www.securityworldmarket.com/int/News/Business-News/secure-vpn-usage-sees-major-uptick-in-russia1.

151 Roskomsvoboda, VPN в России: от блокировки сервисов к блокировке протоколов, 14 November 2023, https://roskomsvoboda.org/en/post/vpn-in-russia-2023/.

152 Advertisement by a VPN provider, which quickly implemented new VPN protocols to bypass Roskomnadzor bans on an internet provider level, 5 September 2023.

153 Alon Nachmany, How Russia's new certificate authority could change the internet in America, *CPO Magazine*, 3 May 2022, https://www.cpomagazine.com/cyber-security/how-russias-new-certificate-authority-could-change-the-internet-in-america/.

154 X.509 infrastructure is a standardized system for creating and managing digital certificates, which work like online identity cards that help websites and services prove they are legitimate and secure. See Using GOST R 34.10-2012 and GOST R 34.11-2012 algorithms with the internet X.509 public key infrastructure, Internet Engineering Task Force, 21 March 2022, https://datatracker.ietf.org/doc/rfc9215/.

155 Получено заключение ФСБ на исполнения КриптоАРМ, Trusted.Ru, 28 January 2021, https://trusted.ru/company/news/zaklyuchenie-fsb-na-kriptoarm/. Further details on their accredations from the FSB for TLS certificates can be found at: Сертификация в ФСБ КриптоПро CSP 5.0 R3 в исполнении base и КриптоАРМ ГОСТ 3, Cryptostore.ru, https://cryptostore.ru/article/novosti/sertifikatsiya_v_fsb_kriptopro_csp_5_0_r3_v_ispolnenii_base_i_kriptoarm_gost_3_/.

156 Национальные сертификаты безопасности сайтов используют только 30% россиян, *Vedomosti*, 16 June 2023, https://www.vedomosti.ru/technology/articles/2023/06/16/980929-sertifikati-ispolzuyut-30.

157 Michael Hill, Traffic interception and MitM attacks among security risks of Russian TLS certs, CSO Online, 15 March 2022, https://www.csoonline.com/article/572235/traffic-interception-and-mitm-attacks-among-security-risks-of-russian-tls-certs.html.

158 Власти Казахстана снова принуждают пользователей устанавливать сертификат, чтобы читать зашифрованную переписку, Khabr, 7 December 2020, https://habr.com/ru/news/531642/.

159 Pjotr Sauer, Shaun Walker and Andrew Roth, Putin questions Ukraine ceasefire plan and sets out string of conditions, *The Guardian*, 13 March 2025, https://www.theguardian.com/world/2025/mar/13/russia-wary-of-proposed-ukraine-ceasefire-plan-as-us-talks-begin. For updates, see: Institute for the Study of War, https://www.understandingwar.org/.

160 IT-компании экспортируют сотрудников, *Kommersant*, 28 February 2022, https://www.kommersant.ru/doc/5237954.

161 Eray Kalelioğlu and Savaştan Kaçan Rus Hackerlar, *Türkiye'ye göç etti: bizim üzerimizden dünyaya saldırıyorlar!*, Webtekno, 12 September 2023, https://www.webtekno.com/savastan-kacan-rus-hackerlar-turkiye-goc-etti-h137197.html.

162 See Misha Glenny, *DarkMarket: How Hackers Became the New Mafia*, New York: Vintage Books, 2012.

163 Отсрочка от весеннего призыва на срочную службу для сотрудников ИТ-компаний, Gosuslugi, 6 February 2024, https://www.gosuslugi.ru/armydelay.

164 Минцифры предложило льготную ипотеку и отсрочку от призыва для айтишников, RBC, 28 February 2022, https://www.rbc.ru/technology_and_media/28/02/2022/621cfacc9a79479492100cfc.

165 Interview with a cyberwarfare specialist, 18 April 2024.

166 Russia's ransomware arrests send dangerous message, *The Washington Post*, 21 January 2021, https://www.washingtonpost.com/opinions/2022/01/21/russias-ransomware-arrests-send-dangerous-message/.

167 Interview with an expert on Eastern European cybercrime, 25 April 2024.

168 US Department of Justice, Alleged operator of Kelihos botnet extradited from Spain, 2 February 2018, https://www.justice.gov/opa/pr/alleged-operator-kelihos-botnet-extradited-spain.

169 Interview with the director of cybercrime investigation for a South-Eastern European nation, 18 April 2024.

170 Conti's blockchain plans: an ominous prospect, NCC Group, 7 July 2022, https://www.nccgroup.com/us/contis-blockchain-plans-an-ominous-prospect/.

171 Andres Einmann, Украинские мошеннические колл-центры активно вербуют жителей Эстонии, *Postimees*, 8 November 2024, https://rus.postimees.ee/8131048/

GLOBAL INITIATIVE
AGAINST TRANSNATIONAL ORGANIZED CRIME

ABOUT THE GLOBAL INITIATIVE

The Global Initiative Against Transnational Organized Crime is a global network with over 700 Network Experts around the world. The Global Initiative provides a platform to promote greater debate and innovative approaches as the building blocks to an inclusive global strategy against organized crime.

www.globalinitiative.net