UKRAINE

Digital Threat Landscape: Civil Society & Media

Internews
Local voices. Global change.

Digital
Security
Lab

Table of Contents

Background

Russia's invasion of Ukraine put significant pressure on the ability of Ukrainian civil society and the media organizations to operate freely and securely. Their digital security is no exception, and the war has exacerbated an already significant problem. This report was prepared by Internews' Internet Freedom & Resilience team under a stream of work which strengthens civil society organizations (CSOs), journalists, and other human rights defenders (HRD) ability to detect, analyze, and build resilience to digital attacks through localized expertise in threat analysis and incident response. This report is intended to provide an overview of the digital threats faced by civil society and media organizations in Ukraine and provide guidance for digital safety experts supporting this community. It is also intended to provide context for the cybersecurity industry which may need to analyze security incidents affecting Ukrainian civil society and media. We conclude with a discussion of mitigation measures that can be proposed by digital security experts to the organizations with whom they work, as well as for civil society and media organizations to implement.

This report was written in close collaboration with Digital Security Lab Ukraine, an organization working to help Ukrainian journalists, human rights defenders, and public activists solve problems in digital security, as well as promote the realization of human rights on the Internet by influencing government policy in the field of digital rights.

The threats, trends, and case studies highlighted in this report were identified through direct digital safety support for at-risk communities (provided by Internews and Digital Security Lab Ukraine), desk research, and conversations with trusted members of the Internet Freedom community. This report aggregates data from incident response work and documents attack patterns specific to Ukraine.

October 2023

Written and Edited: Martijn Grooten, Ashley Fowler, Marc Shaffer, and Skyler Sallick
Copyediting, Design, and Layout: Skyler Sallick

Digital Threat Landscape

Political Context, Civil Society, and the Media

While Ukraine is an electoral democracy, the country's democratic institutions are fragile due to the ongoing war with Russia.[1] The current president, Volodymyr Zelensky, was elected by competitive election in 2019 and discussed the possibility of holding the next constitutionally mandated presidential election in 2024 amidst the conflict.[2] Opposition politicians and some members of civil society have criticized the plan to hold the election as the logistical challenge could prevent full participation. There is also concern that the election would serve to entrench Zelensky without the opportunity for true opposition.[3] In 2023, the Economist's Democracy Index categorized Ukraine as a "Hybrid Regime," scoring 5.42 out of 10.[4] The country is rated as "Partly Free" in Freedom House's 2023 Freedom in the World report, scoring 50 out of 100.[5] Freedom House marks Ukraine's 19 point fall from their previous year's rating, noting that "The Russian military's full-scale invasion of Ukraine in February 2022 led to significant deterioration in the political rights and civil liberties enjoyed by Ukrainians."[6] Following the outbreak of war with Russia, President Zelensky enacted Martial Law which permits restrictions on constitutionally protected rights such as freedom of speech, the right to elect and be elected, and the right to peaceful assembly and strike.[7] At the time of writing, Ukraine remains under Martial Law.

Despite the challenges of war, Ukrainian civil society has demonstrated resilience in their ability to recruit volunteer networks, raise funds to support relief efforts for citizens, and document evidence of Russian war crimes.

According to Freedom House, civil society remains robust and effective, strengthening their role as key stakeholders in the country's reform efforts.[8] Prior to war with Russia, Ukrainian oligarchs exerted significant influence over the political sphere, exacerbated by widespread corruption.[9] While oligarchic power has decreased as a result of the war, corruption remains a present issue that hampers political progress.[10] Under Martial Law, civil society organizations face legislative reforms that impact the ease with which they can operate. Namely, civil society organizations are no longer permitted to use foreign bank transactions.[11] Despite the challenges of war, Ukrainian civil society has demonstrated resilience in their ability to recruit volunteer networks, raise funds to support relief efforts for citizens, and document evidence of Russian war crimes.[12]

In times of war, information is currency and government restrictions under Martial Law reflect that reality. In March 2022, the National Security and Defense Council of Ukraine (NSDC) issued a set of wartime media regulations that initially received widespread support as they were deemed appropriate amidst war. However, overtime, many have grown to see these restrictions as an encroachment on Ukraine's democratic rights.[13] These restrictions and the ultimate "Law on Media" are complicated by Ukraine's EU Candidacy as the country is now required to meet certain media reform obligations to maintain candidacy status. Ukrainian lawmakers and civil society continue to grapple with the delicate balance of restrictive wartime necessities and expanding democratic institutions in the country's legislative reform process. In this regard, Digital Security Lab Ukraine remarks that "Some of these amendments are aimed at improving the state of affairs with human rights in media and digital environments, while others can do more harm than good under the disguise of national security protection and martial law."[14]

Outside the legislative pressures created by Martial Law, civil society currently faces significant financial and physical security challenges. Although maintaining operations under difficult circumstances, many Ukrainian civil society organizations are currently operating under conditions of financial instability, and this has become increasingly threatening as the war continues. In 2022, 82% of CSOs focused on women's rights reported a lack of financial resources.[15] In the occupied territories, activists face persecution and capture by Russian military. In most cases, Russian forces targeted individuals due to activist participation in marches or protests against occupying forces.[16]

Many Ukrainian civil society organizations are currently operating under conditions of financial instability, and this has become increasingly threatening as the war continues.

Cybersecurity in Ukraine

Ukraine has historically been one of the main countries from which cybercriminals operate. Though there have been a number of arrests over the years, such as the ringleaders of ZueS[17] and Carberp[18] banking malware, Ukraine has previously been thought of as a "cyber safe haven"[19] for criminal activity. The freedom with which cybercriminals operate in the country has been attributed to Ukraine's decade long focus on countering Russian aggression. Ukraine's national Computer Emergency Support Team, CERT-UA, was accused of being ineffective against cybercrime as a result of the "almost exclusive current focus on fighting Russian aggression in eastern Ukraine" following Russia's 2014 annexation of Crimea.[20] The career of cybercriminal-turned-politician Dmitri Golubov, member of Ukrainian Parliament from 2014 to 2019, is illustrative of the freedom with which cybercriminals operate.[21]

Cybercrime in Ukraine and Russia has long been interwoven, with many actors operating in both countries. It is common for malware made in the region to check for the presence of Russian or Ukrainian keyboards (or one of several other countries in the region) and not proceed with malicious activities if one was detected: this would prevent upsetting local authorities.[22]

However, things changed following the full-scale military invasion of Ukraine in 2022. Cybercriminals in both countries declared their loyalty to their respective governments, leading to the breakup of several criminal groups. This was seen most publicly with the Conti ransomware gang, whose Russian members publicly stated their support for the Russian invasion,[23] after which a Ukrainian member published some 60,000 internal chat messages, showing the internal operations of the group.[24] Google's Threat Analysis Group believes that, since then, some of the group's former Russian members have offered their skills to the government.[25]

However, things changed following the full-scale military invasion of Ukraine in 2022. Cybercriminals in both countries declared their loyalty to their respective governments, leading to the breakup of several criminal groups.

Russian targeting of Ukraine increased following the invasion of Crimea. In December 2015, residents in the Ivano-Frankivsk region in Western Ukraine faced electricity blackouts lasting one to six hours, after a hack penetrated the country's power grid, the first attack specifically targeting a foreign country's electrical supply.[26] The hack is generally believed to be the work of a group referred to as Sandworm– the cyberwarfare unit of the GRU, Russia's military intelligence service. Sandworm is also thought to be behind a second, shorter, power outage in Kyiv in 2016[27] and a failed attempt to cause a third outage in April 2022, shortly after the full-scale invasion.[28]

In June 2017, Sandworm hackers managed to infiltrate a small company that created a widely used Ukrainian tax accounting software package, pushing a rogue update to its customers around the world. The update contained the NotPetya malware which encrypts all files on infected computers. Although NotPetya masquerades as ransomware, it is ultimately destructive in nature as there is no method to decrypt files. With many global companies affected, the total damage was estimated to exceed $10 million USD.[29]

Various "hacktivist" (activist hacker) groups also target Ukraine and its supporters, such as Cyber Berkut,[30] Killnet, and NoName057(16).[31] Other prominent Russia-linked actors include Gamaredon, which appears to exclusively target Ukraine, and APT28 (Fancy Bear), another group associated with the GRU that has conducted various attacks on Ukrainian targets.[32] In 2022, APT28 (Fancy Bear) conducted a phishing campaign targeting users of the UKR.NET webmail service, which is popular among Ukrainian civil society organizations.[33] Russia-linked actors have increasingly targeted Ukraine since Russia's annexation of Crimea in 2014, leading some to call the country "Russia's playground" when it comes to cyber-attacks.[34]

Ukraine has also created an environment conducive to the experimentation of multistakeholder cooperation around cybersecurity and cyberdefense. Starting with the Russian annexation of Crimea and especially since the start of the full-scale war in 2022, Ukraine has received a lot of support for its cyber defense, from both foreign governments and the private sector. This support has included free software and services, rapid sharing of information and measures to provide business continuity in case of seizure[35] of physical assets.

The State of Cybersecurity of Civil Society and Media

Russia's war in Ukraine changed the digital threat landscape of the country's civil society and independent media. Prior to the war, journalists worried about cyberattacks such as hacks or digital harassment by politicians whose corruption they wished to expose. Following the invasion, such threats decreased as the country was unified by a common enemy. However, local digital security experts report the resumption of small-scale internal hacking activity as the war progresses.

There are few known instances of explicit digital targeting of Ukrainian civil society by Russian or Russian-linked actors. While such attacks may occur undetected, it may also be that Russian actors are more focused on Ukrainian government and military targets at this time.[36] However, as the line between civil society and government is sometimes blurred, Ukrainian civil society can suffer as "collateral damage" when government institutions face digital threats. Regardless of the current geopolitical situation in the country, indiscriminate cybercrime continues to target users through phishing and malware attacks, and members of civil society are sometimes on the receiving end of such attacks.

Many journalists and CSOs that receive suspicious emails understand the dangers, often forwarding them to organizations like DSLU for analysis. Although, cyber hygiene among Ukrainian civil society is far from perfect as there is widespread use of cracked versions of legitimate software which often contains malware.[37] Given the amount of free software licenses sent to Ukrainian entities, the widespread use of cracked software may be surprising to some. However, IT administrators at government departments and civil society organizations report that it is often easier to install cracked software than navigate the bureaucratic hurdles surrounding access to these free licenses.

While Ukraine has attempted to acquire Pegasus for its own use since at least 2019, the Israeli government blocked NGO Group from selling their software to Ukraine.

There are no known instances of advanced mobile malware, such as Pegasus, in Ukraine. While Ukraine has attempted to acquire Pegasus for its own use since at least 2019, the Israeli government blocked NGO Group from selling their software to Ukraine. While no official reason has been offered for their decision to block the sale, experts believe this is due to a close intelligence relationship between Israel and Russia. Based on previous decisions, Israel's government is wary of upsetting Russia and likely fear that Ukraine will use Pegasus against Russian officials, which was explicitly banned in the sale of Pegasus to the Estonian government.[38]

Mitigation Measures

Account security is important for anyone in Ukraine, but crucial for members of civil society. **Two-factor authentication is a must** – and mitigates the use of weak and/or reused passwords. Though better than no two-factor authentication at all, SMS shouldn't be considered secure, especially for at-risk users. Using an authentication app is better than SMS, and using a hardware token generally provides the best security, although this requires additional equipment.

Some messaging apps such as Telegram, WhatsApp, and Signal, require the use of a phone number to activate the account. Enabling two-factor authentication involves **adding a passcode** in addition to using SMS to access the account, providing security in cases of SMS compromise. When this feature is enabled, the app will periodically ask the user to input their passcode to ensure the messages are not being accessed by someone besides the owner of the account. This prevents account takeover through SMS interception, which is common in the country.

Endpoints, such as laptops and mobile phones, should be kept up to date by applying security patches to operating systems and other software whenever they become available. **Software should only be acquired from official sources.** In many cases, this requires payment. NGOs should not be shy to discuss this with funders, or to look for free alternatives such as open-source software and programs that provide software free of cost or at reduced prices to eligible NGOs.

There is no evidence of advanced spyware or malware being used to target civil society or the media in Ukraine, but given the war with Russia, one of the most powerful "cyber powers" in the world, the possibility should not be excluded. This is particularly true for those living and working in parts of the country controlled by Russia.

Members of civil society and journalists should be vigilant and implement common practices, such as **regularly rebooting phones** – which would mitigate the risk of advanced spyware – **using Google's Advanced Protection Program on Google accounts and Lockdown Mode on iPhones and iPads**. Suspicious email attachments or links should not be opened or clicked on, rather they should be forwarded to trusted experts for examination such as DSLU.

Those in Russian occupied parts of the country may want to **use VPNs to evade censorship** and interference by the occupying authorities. However, those whose activities puts them at risk of arrest or harassment should be aware that using a VPN (or Tor) would make their traffic stand out within the community and may draw unwanted attention.

Russian made devices, which connect to Russian servers, are common in Ukraine. Although the risks associated with these connections vary by device, they are best avoided. At the time of writing this report, Internet connections to Russia are blocked in Ukraine, and these Russian made devices need VPNs to connect to the Russian servers. While using VPNs to avoid government censorship is generally a good idea and recommended in Russian-controlled territory, in this context, needing a VPN to connect can serve as a warning that the device is connecting to a server in Russia.

Case Studies

Remcos RAT Targeting Ukraine

In February 2023, two separate non-governmental organizations (NGOs) in Ukraine received a phishing email with the same password-protected archive attached to it. Instead of opening the attachment, the individuals forwarded the email for analysis to DSLU, an organization working to help Ukrainian journalists, human rights defenders, and public activists solve problems in digital security.

While the archive was relatively small, the decompressed file inside the archive was a very large Windows executable (.exe) file (657MB). The file size prevented DSLU from uploading it to VirusTotal, a popular Google-owned site for threat intelligence, as the site has a file limit of 650MB. The large size of the archive and password-protection are designed to help the file bypass first-layer security defences such as an anti-virus or email security product when opened by the user. Inflated file size and the use of password-protected archives are common anti-analysis techniques in targeted and non-targeted malware attacks.

Using Detect-It-Easy, a tool that helps analysts determine file types, DSLU learned that the file was obfuscated using the SmartAssembly obfuscator– another common anti-analysis technique. However, through the use of the .NET deobfuscator de4dot, DSLU was able to create a version of the file that was less than 0.1% of the original size with the exact same functionality. This file was uploaded to VirusTotal. DSLU also analysed the file in Flare VM, a Windows-based security distribution managed by security company Mandiant.[39]

Through this analysis, DSLU determined that the file was compiled on February 20th, 2023, right before the emails were sent. The dynamic analysis performed in Flare VM showed that the file was set up to store a copy of itself on the disk and run while adding a key to the Windows registry, ensuring the executable would run every time the computer started up. While this is a technique used by legitimate programs, it is also a very common strategy that allows malware to maintain presence on an infected Windows computer after a reboot.

During their analysis, DSLU also found the program connecting to two IP addresses on the Internet. Analyzing the IP addresses a malware sample connects to can be used to link it to previously seen campaigns, allowing for a better understanding of the malware. By using Process Hacker, a tool used to monitor system resources and debug malware, the analysts were able to detect 12 other IP addresses the malware might connect to. They also noted the string "Remcos Agent initialized" and other references to Remcos.

Based on the results of using the tools previously discussed and various malware sandboxes, the analysts concluded that this attack was likely a variant of the Remcos Remote Access Trojan (RAT). A RAT gives an operator full remote access to an infected computer, making it an ideal tool for both espionage and committing financial fraud. Remcos was first analysed in February 2017 and is among the most commonly detected RATs.[40] Many RATs are sold on the cybercrime black market, and some – Remcos being one of them – were originally developed as a Remote Access *Tool* to provide remote access for support purposes.

It is unclear why the two NGOs were targeted with Remcos. It may have been an opportunistic attempt at indiscriminate cybercrime, and it may also have been a more targeted threat by an actor interested in their activities. Moderately advanced actors operating on behalf of nation states sometimes purchase their attack tools from cybercriminals rather than develop their own.

In either case, not opening the attachment prevented this attack from being successful, while forwarding the email to DSLU helped the community better understand the threat. This case study demonstrates why it is advantageous for an organization in the local community, such as DSLU, to possess threat analysis skills. Lessons learned from this investigation can inform trainings and continued support for at-risk communities, allowing experts to tailor their mitigations and recommendations to the changing threat landscapes.

Possible Gamaredon Malware Targeting Local Government Official

An individual employed by a Ukrainian governmental agency with previous experience at a civil society organization received an email that contained an attachment sent from a compromised local government account. Instead of opening the attachment, the recipient forwarded the email for analysis to DSLU, an organization working to help Ukrainian journalists, human rights defenders, and public activists solve digital security problems.

The email contained a HTML attachment that utilized an "HTML smuggling" technique to open a Roshal Archive (RAR) high quality compressed file.[41] The RAR archive contained a .hta file which is the common file extension for an HTML application.[42] HTML applications are used for many legitimate purposes on Windows computers, but their ability to run code makes them popular among malware authors as well. These applications are especially appealing as they run inside the legitimate program mshta.exe, allowing the malware to avoid being flagged by security products. The use of legitimate programs for malicious purposes is referred to as living-off-the-land or LOLbin.

The .hta file in the RAR archive downloaded a payload from the following URL: http://80.90.181[.]243/sb.12.05.gif/query/heal.jpeg. Despite the contents of the URL, the result would not be a GIF or JPEG file, but rather a locally executed PowerShell script. Given that the use of an IP-based URL is not common for legitimate purposes, this was not an advanced attempt to mislead the user. However, the average user is likely to assume that this URL would download an image. Additional emails that were later attributed to the same campaign used different file paths but downloaded the same payload.

Interestingly, the payload would only download when contacted from a Ukrainian IP address, which suggests geographic targeting of the email. This meant that opening the attachment in a sandbox would not result in any further activity. The DSLU analysts had to run the file in a virtual machine locally to complete the analysis.

PowerShell is a scripting language included in Windows and is a powerful tool for legitimate and malicious purposes alike. In this case, the script set a run key, opened an empty Word document, and created a local file named "junior." Opening a Word document could be an anti-analysis technique as the malware would not run without Microsoft Word installed, which could be the case for some analysis environments.

The "junior" file used two methods to obtain the IP address of the command-and-control server: it connected to a public Telegram channel or, as a backup, used a domain name. The use of cloud services and Telegram for malware to obtain command and control servers is a widely used technique, potentially providing greater resilience than the use of domain names or hardcoded IP addresses. This technique means that actors don't have to obtain or register servers in advance and can do so after the campaign has begun.

After obtaining the command-and-control server's address, an HTTP GET request is sent to the server containing the machine name and hard drive serial number in the User-Agent header field. While the program likely expects a response, nothing but 404 responses were observed during analysis. It could be that the server was somehow detecting it was being contacted from an analysis machine.

Although the analysis did not detect malicious activity, many aspects of the observed behaviour indicate that this was indeed malware. For a small organization like DSLU, linking a campaign to a particular actor with a high degree of certainty is often impossible as it requires large telemetry. However, many artefacts of this malware – the use of .hta files, PowerScript, and Telegram to obtain the C&C server – as well as the targeting of Ukraine suggests the work of a threat actor security companies refer to as Gamaredon (other names for this group include Primitive Bear and Shuckworm).[43]

Gamaredon is a Russia-linked cyber-espionage group that has demonstrated a particular focus on Ukraine since its detection in 2013. Its targets have included government organisations, law enforcement, and NGOs.

Further Reading

As seen in this report, civil society organizations and journalists often face unique, advanced threats, while lacking the resources to detect, analyze, and prevent them. An in-depth understanding of the threats facing civil society and media allows digital security practitioners to tailor their responses and better support the organizations they work with, leading to customized mitigation measures that are more effective and easier for civil society and media organizations to implement. For more information on the threats faced by civil society and journalists, Internews and their partners have authored the report "Global Trends in Digital Threats: Civil Society & Media," as well as Digital for Armenia, Brazil, Serbia, and Ukraine. These resources can be found on the Internews' Technology Resources webpage.

History of Ukraine

Ukraine (Україна) is the second largest country in Europe bordered by Russia, Belarus, Poland, Slovakia, Hungary, Romania, and Moldova. Ukraine has coastline along the Black Sea and the Sea of Azov. The country is a unitary republic with one legislative body and is a member of the United Nations,[44] the World Trade Organization,[45] the Council of Europe,[46] and the Organization for Security and Cooperation in Europe.[47] In February 2022, Russia invaded Ukraine, and as of the writing of this report, the war is still being fought.

Slavic peoples settled in the area that is now Ukraine in the fourth century CE, with Kyiv becoming the main town.[48] In the ninth century, the area around Kyiv was consolidated into a state called the Kievan Rus. The Kievan Rus became a dominant power, reaching its peak in the 11th century.[49] The Kievan Rus is an important aspect of Eastern European history, as Russia, Ukraine, and Belarus all tie their national identities to the early medieval state. In Ukrainian nationalist historiography, the Kievan Rus is "an essentially Ukrainian state and claims that the differences between Russians and Ukrainians were apparent and quite profound even then."[50] In contrast, Russian imperialist historians used the Kievan Rus to justify Ukrainians and Belarusians as "mere subgroups."[51] This tension continues to influence the relations between the countries, as seen in Putin's repeated invocations of the Kievan Rus to this day.[52]

After the collapse of the Kievan Rus state, control of Ukrainian territory was alternately dominated by Lithuania, Poland, Russia, and the Hetmanate – a Cossack self-governing territory. In the 18th century, the Russian empire consolidated control over Ukraine and largely maintained this rule until the collapse of the Soviet Union.[53] In the 19th century, Ukrainians, along with several other European regions, began developing a sense of nationalism and the belief in self-determination. At the time, Ukrainian's homeland was divided between Russia in the east and the Austro-Hungarian Empire in the west. These two empires responded differently to the movement, with increased recognition of minorities in the regions under Austria and a crackdown on Ukrainian identity under Russian. After the overthrow of the Russian monarchy, Ukraine briefly declared independence before the Russian civil war led to the incorporation of Ukraine into the Soviet Union as the constituent Ukrainian Soviet Socialist Republic, which did not have political autonomy.[54] Under Josef Stalin's policy of collectivization, Soviet leaders engineered a famine in Ukraine called the Holodomor that led to the deaths of millions of Ukrainians.[55]

Ukraine's history of resistance against Russian control has been significant in the past century, continuing into the period of open war. In 1991, Ukraine gained independence and adopted its current constitution in 1996. The country experienced a recession between 1991 and 1999 during the transition to a market economy, losing 60% of its GDP and experiencing hyperinflation that reached a peak of 100,000% in 1993. Since the 1990s, Ukrainians have revolted against the government twice, with the Orange Revolution against the disputed election of 2004 and again during Kyiv's Maidan protests that toppled the pro-Russian government in 2014. Under the interim government, Russian troops invaded the Crimean Peninsula and annexed the territory. Since then, Russian-backed separatist militias in eastern Ukraine fought against government forces and declared independence.[56] The tension culminated with the Russian invasion in 2022.[57]

Acknowledgements

Since 2021, Internews has worked with seven Threat Labs (*local organizations with the technical capacity and appropriate tools to analyze suspicious phishing and malware samples and then share information back to the community regarding attack trends, emerging threats, and countermeasures*) to respond to incidents affecting the digital security of civil society and media organizations around the world. The data collected through the incident response program helped shape mitigations and response approaches for at-risk communities and informed this report.

Internews would like to express our gratitude to the community of Threat Labs that worked with us on this project. They are committed to assisting those in need and ensuring that their partners in civil society and media organizations can complete their important work safely and effectively. In total, this project supported Threat Labs in responding to over 200 digital security incidents and publishing over 60 educational resources through their websites and social media platforms.

Special thanks to Digital Security Lab Ukraine for providing the information to document and share these case studies and for reviewing and contributing valuable feedback to this report. The report would not have been possible without their support.

Endnotes

[1] "Nations in Transit Methodology." Freedom House. Accessed August 2023. https://freedomhouse.org/reports/nations-transit/nations-transit-methodology.; "Nations in Transit 2023: Ukraine." Freedom House. Access August 2023. https://freedomhouse.org/country/ukraine/nations-transit/2023.

[2] Starkov, Nick. "Zelenskiy says elections could happen under fire if West helps." *Reuters*. Last modified August 27, 2023. https://www.reuters.com/world/europe/zelenskiy-says-elections-could-happen-under-fire-if-west-helps-2023-08-27/.

[3] Kramer, Andrew E. "Zelensky's First Term Is Almost Up. No One's Sure What Happens Next." The New York Times. October 5, 2023. https://www.nytimes.com/2023/10/05/world/europe/ukraine-zelensky-elections-war.html

[4] "Democracy Index 2022: Frontline democracy and the battle for Ukraine," Economist Intelligence. Page 9.

[5] "Freedom in the World 2023: Ukraine." Freedom House. Access August 2023. https://freedomhouse.org/country/ukraine/freedom-world/2023.

[6] "Freedom in the World 2023: Ukraine," Freedom House.

[7] "Nations in Transit 2023: Ukraine," Freedom House.

[8] "Freedom in the World 2023: Ukraine," Freedom House; "Nations in Transit 2023: Ukraine," Freedom House.

[9] "Freedom in the World 2023: Ukraine," Freedom House.

[10] "Freedom in the World 2023: Ukraine," Freedom House.

[11] "Freedom in the World 2023: Ukraine," Freedom House.

[12] "One year into Russia's war on Ukraine: Civil society in the crossfire." Civicus Lens. Last modified February 24, 2023. https://lens.civicus.org/one-year-into-russias-war-on-ukraine-civil-society-in-the-crossfire/.

[13] "Nations in Transit 2023: Ukraine," Freedom House.

[14] "DSLU launches a monthly digest on media and digital rights regulation in Ukraine." DSLU. Accessed September 2023. https://freespeech.dslua.org/dslu-launches-a-monthly-digest-on-media-and-digital-rights-regulation-in-ukraine/.

[15] "Nations in Transit 2023: Ukraine," Freedom House.

[16] "Nations in Transit 2023: Ukraine," Freedom House.

[17] Gallagher, Sean. "Alleged botnet mastermind and his coders busted by Russian, Ukrainian security." ARS Technica. April 4, 2013. https://arstechnica.com/tech-policy/2013/04/alleged-botnet-mastermind-and-his-coders-busted-by-russian-ukranian-security/.

[18] Gallagher, "Alleged botnet mastermind and his coders busted by Russian, Ukrainian security."

[19] Kostyuk, Nadiya. "Ukraine: A Cyber Safe Haven?" In *Cyber War in Perspective: Russian Aggression Against Ukraine*, edited by Kenneth Geers, 113 – 122. Tallinn, Estonia: NATO CCD COE Publications, 2015. https://www.ccdcoe.org/uploads/2018/10/Ch13_CyberWarinPerspective_Kostyuk.pdf.

[20] Kostyuk, "Ukraine: A Cyber Safe Haven?"

[21] "Dmitri Golubov (politician)." *Wikipedia*. Accessed September 2023. https://en.wikipedia.org/wiki/Dmitri_Golubov_(politician).

[22] "Try This One Weird Trick Russian Hackers Hate." KrebsonSecurity. May 17, 2021. https://krebsonsecurity.com/2021/05/try-this-one-weird-trick-russian-hackers-hate/.

[23] Abrams, Lawrence. "Conti ransomware's internal chats leaked after siding with Russia." *Bleeping Computer*. February 27, 2022. https://www.bleepingcomputer.com/news/security/conti-ransomwares-internal-chats-leaked-after-siding-with-russia/.

[24] Bing, Christopher. "Russia-based ransomware group Conti issues warning to Kremlin foes." *Reuters*. February 25, 2022. https://www.reuters.com/technology/russia-based-ransomware-group-conti-issues-warning-kremlin-foes-2022-02-25/.

[25] Huntley, Shane. "Fog of war: how the Ukraine conflict transformed the cyber threat landscape." Google, Updates from Threat Analysis Group. February 16, 2023. https://blog.google/threat-analysis-group/fog-of-war-how-the-ukraine-conflict-transformed-the-cyber-threat-landscape/.

[26] Zetter, Kim. "Inside the Cunning, Unprecedented Hack of Ukraine's Power Grid." *Wired*. March 3, 2016. https://www.wired.com/2016/03/inside-cunning-unprecedented-hack-ukraines-power-grid/.

[27] Greenberg, Andy. "How an Entire Nation Became Russia's Test Lab for Cyberwar." *Wired*. June 20, 2017. https://www.wired.com/story/russian-hackers-attack-ukraine/.

[28] Greenberg, Andy. "Russia's Sandworm Hackers Attempted a Third Blackout in Ukraine." *Wired*. April 17, 2022. https://www.wired.com/story/sandworm-russia-ukraine-blackout-gru/.

[29] Greenberg, Andy. "The Untold Story of NotPetya, the Most Devastating Cyberattack in History." *Wired*. August 22, 2018. https://www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world/.

[30] Rodrigo, "Cyber Berkut Graduates From DDoS Stunts to Purveyor of Cyber Attack Tools." Recorded Future. June 8, 2015. https://www.recordedfuture.com/cyber-berkut-analysis.

[31] "Pro-Russian Hacktivist Groups Target Ukraine Supporters." Intel471. September 14, 2022. https://intel471.com/blog/pro-russian-hacktivist-groups-target-ukraine-supporters.

[32] Kremez, Vitali. "Pro-Russian CyberSpy Gmaredon Intensifies Ukrainian Security Targeting." SentinelLABS. February 5, 2020. https://www.sentinelone.com/labs/pro-russian-cyberspy-gamaredon-intensifies-ukrainian-security-targeting/.

[33] Aimé, Felix. "APT28 leverages multiple phishing techniques to target Ukrainian civil society." Sekoia blog. May 17, 2023. https://blog.sekoia.io/apt28-leverages-multiple-phishing-techniques-to-target-ukrainian-civil-society/.

[34] Cerulus, Laurens. "How Ukraine became a test bed for cyberweaponry." *Politico*. February 14, 2019. https://www.politico.eu/article/ukraine-cyber-war-frontline-russia-malware-attacks/.

[35] Beecroft, Ben. "Evaluating the International Support to Ukraine Cyber Defense." Carnegie Endowment for International Peace. November 3, 2022. https://carnegieendowment.org/2022/11/03/evaluating-international-support-to-ukrainian-cyber-defense-pub-88322.

[36] Nimmo, Ben and David Agranovich. "Meta's Adversarial Threat Report, Second Quarter 2022." Meta. August 4, 2022. https://about.fb.com/news/2022/08/metas-adversarial-threat-report-q2-2022/.

[37] Abrams, Lawrence. "Pirated Software is All Fund and Games Until Your Data is Stolen." *Bleeping Computer*. February 2, 2020. https://www.bleepingcomputer.com/news/security/pirated-software-is-all-fun-and-games-until-your-data-s-stolen/.

[38] Kirchgaessner, Stephanie. "Israel blocked Ukraine from buying Pegasus spyware, fearing Russia's anger." *The Guardian*. March 23, 2022. https://www.theguardian.com/world/2022/mar/23/israel-ukraine-pegasus-spyware-russia.

[39] Kacherginsky, Peter. "FLARE VM: The Windows Malware Analysis Distribution You've Always Needed!" Mandiant. July 26, 2017. https://www.mandiant.com/resources/blog/flare-vm-the-windows-malware.

[40] Bacurio, Floser and Joie Salvio. “REMCOS: A New RAT In The Wild.” FORTINET. February 14, 2017. https://www.fortinet.com/blog/threat-research/remcos-a-new-rat-in-the-wild-2.

[41] Microsoft Threat Intelligence. “HTML smuggling surges: Highly evasive loader technique increasingly used in banking malware, targeted attacks.” Microsoft. Novembre 11, 2021. https://www.microsoft.com/en-us/security/blog/2021/11/11/html-smuggling-surges-highly-evasive-loader-technique-increasingly-used-in-banking-malware-targeted-attacks/.

[42] “HTML Application.” *Wikipedia*. Accessed September 2023. https://en.wikipedia.org/wiki/HTML_Application.

[43] “Gamaredon Group.” MITRE. Last modified March 22, 2023. https://attack.mitre.org/groups/G0047/.

[44] “Member States.” United Nations. Accessed September 2023. https://www.un.org/en/about-us/member-states.

[45] “Members and Observers.” World Trade Organization. Accessed September 2023. https://www.wto.org/english/thewto_e/whatis_e/tif_e/org6_e.htm.

[46] “46 Member States.” Council of Europe. Accessed September 2023. https://www.coe.int/en/web/portal/46-members-states.

[47] “Participating States.” Organization for Security and Co-operation in Europe.” Accessed September 2023. https://www.osce.org/participating-states.

[48] “Ukraine summary.” *Britannica*. Accessed September 2023. https://www.britannica.com/summary/Ukraine.

[49] “Kievan Rus.” *Britannica*. Last modified August 11, 2023. https://www.britannica.com/topic/Kyivan-Rus.

[50] Polkhy, Serhii. *The Origins of the Slavic Nations: Premodern Identities in Russia, Ukraine, and Belarus*. Camridge University Press. Page 65. http://assets.cambridge.org/97805218/64039/excerpt/9780521864039_excerpt.pdf

[51] Ibid.

[52] Andrejsons, Kristaps. “Russia and Ukraine Are Trapped in Medieval Myths.” *Foreign Policy*. February 6, 2022. https://foreignpolicy.com/2022/02/06/russia-and-ukraine-are-trapped-in-medieval-myths/.

[53] “Ukraine summary,” *Britannica*.

[54] “A short history of Ukrainian nationalist—and its tumultuous relationship with Russia.” *The Conversation*. March 17, 2022. https://theconversation.com/a-short-history-of-ukrainian-nationalism-and-its-tumultuous-relationship-with-russia-179346.

[55] “Ukraine summary,” *Britannica*.

[56] Vorobyov, Niko. “Ukraine crisis: Who are the Russia-backed separatists?” Al Jazeera. February 4, 2022. https://www.aljazeera.com/news/2022/2/4/ukraine-crisis-who-are-the-russia-backed-separatists

[57] “Ukraine summary,” *Britannica*.