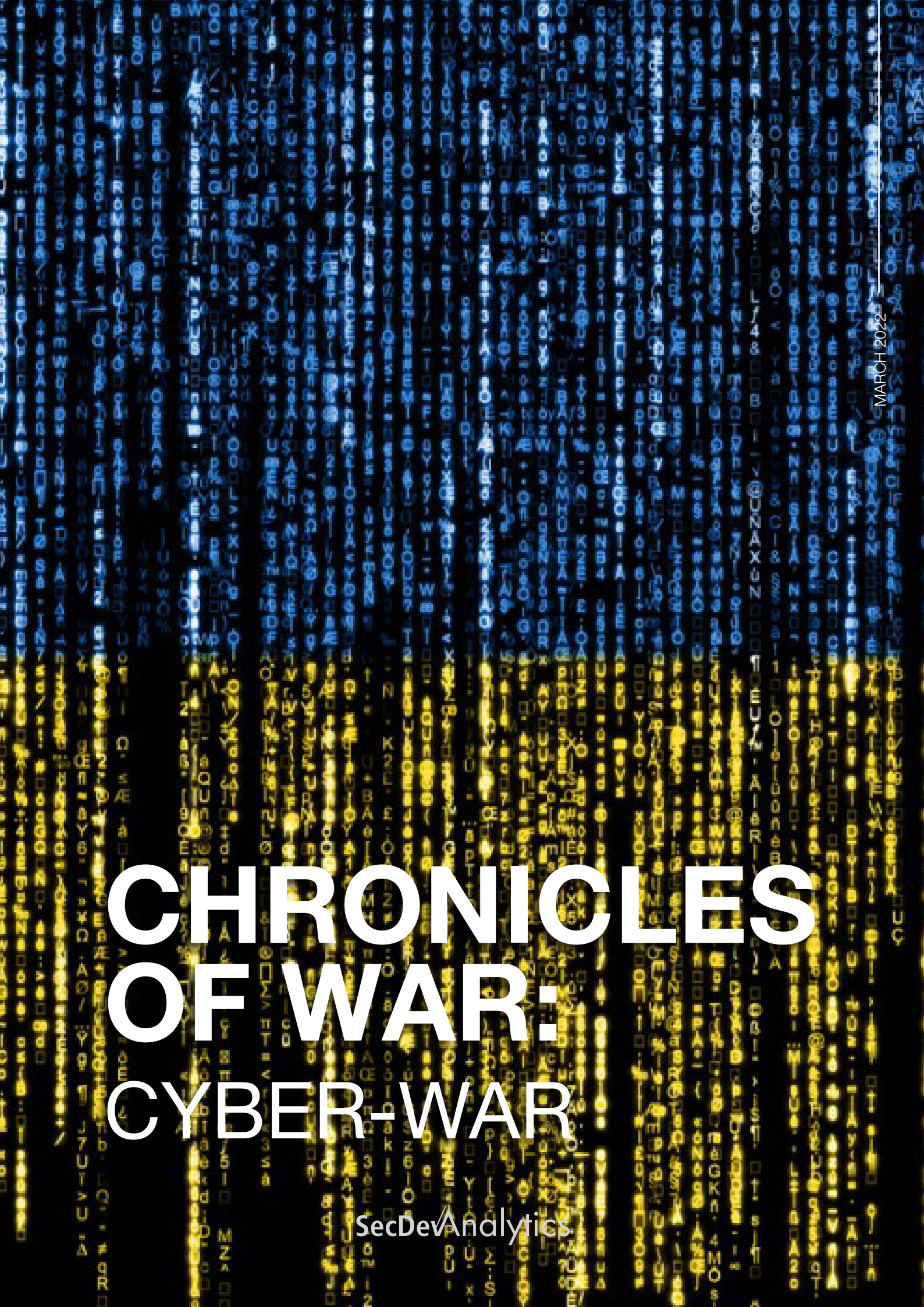

CHRONICLES OF WAR:

CYBER-WAR

SecDevAnalytics

MARCH 2022

Contents

14 March 2022

About the Chronicles of War

The Chronicles of War is an internal SecDev research initiative designed to assess the trajectory of the Russia-Ukraine war during the first month of the war. Relying principally on open sources and key informant interviews in Ukraine and Russia, the focus is on three key areas:

- Security and safety of Ukraine's civilian nuclear infrastructure. The war in Ukraine is the first to occur within a country operating multiple civilian nuclear plants and countless civilian and medical facilities containing radiological materials.
- The cyber dimensions of the Ukraine conflict. Most conflicts now occur in five domains, including cyberspace. The escalatory use of cyberweapons could result in the invocation of NATO Article 5 provisions and pull more countries into the war.
- The perception of fighting by Russian soldiers and civilians. Successful war-fighting often depends on motivated and trained troops and a supportive public. Using digital methods to listen in on soldier conversations and assess wider public sentiment, it is possible to assess the strength, organization and effectiveness of Russia's war effort.

After three weeks of intense fighting, the Russian-Ukraine war is entering a dangerous new phase. War is being waged on land, in the air, on the water and in space. It is also occurring in cyberspace, where attribution and the rules of engagement are often less clear. SecDev Group is tracking trends in cyberwar in Ukraine, Russia and around the world in multiple languages and media outlets. The following summary provides a rapid assessment from notable cyber-related events in the lead-up and initial stages of the war.

Key takeaways

- Cyberwar in Ukraine is occurring across all fronts. Over the past three months Ukrainian government agencies and banks were hit with several types of destructive malware including WhisperGate, HermeticWiper, FoxBlade and IsaacWiper. Many Russian government agencies, media outlets, private companies, influencers and celebrities are also targets of retaliatory hacking.

- Both Ukraine and Russia were supported by a combination of volunteer hacking and cybercrime groups. Ukraine is supported by Anonymous and has appealed to volunteers to engage in cyber operations against Russia. One of the largest groups engaging in hacking against Russia is the IT Army of Ukraine whose channel on Telegram currently has more than 307,500 subscriptions. From the Russian side support is provided by Conti, Stormous, and the Red Bandits, among others.

- Ukrainian civilian digital infrastructure is a key target of cyberattacks. A range of DDOS, phishing and 'wiper' malware attacks were directed against the agriculture sector, emergency response services, humanitarian aid efforts and energy sector organizations and enterprises. These attacks have erased data, compromised accounts and rendered computers and networks inoperable.

- A widening number of countries are also affected by the expanding cyberwar. Belarus was targeted by pro-Ukrainian cyber groups due to its alliance with Russia. Lithuania and Latvia were hit by HermeticWiper, resulting in data being deleted off computers in several governmental organizations. Israel was struck by the country's worst cyber-attack. EU government officials involved in supporting Ukrainian refugees are also targeted by a phishing campaign to gain intelligence on refugee movements. This attack resembles a campaign carried out by Ghostwriter, a hacking group also known as TA445 or UNC1151, which previously supported Belarus.

- A wide range of technology firms are actively involved in monitoring vulnerabilities, focusing particularly on malware targeting Ukraine. Prominent examples include Microsoft, IBM, ESET, Symantec and Avast that are providing threat analysis and intelligence as well as defensive recommendations to the Ukrainian government.

Cyber attacks targeting Ukraine

Russia's cyber campaign against Ukraine began well before the onset of the military invasion that took place on 24 February 2022. NATO members anticipated major offensive engagements from Russia and likewise supported Ukrainian officials for the worst. SecDev Group charted a number of the key headlines associated with Russia's efforts, a shortlist of which is summarized below.

On 15 January 2022, the Microsoft Threat Intelligence Center (MSTIC) warned of a destructive malware used against the Ukrainian government called"WhisperGate". According to Microsoft, the malware first appeared in Ukraine on January 13. The company described it as a possible Master Boot Record (MBR) wiper that disguises itself as ransomware but lacks a ransom recovery mechanism.

A week before Russia's "special military operation", two of the country's banks and its defense ministry were targets of DDoS cyberattacks. Customers of one of the state-owned banks received text messages that the bank's ATMs were not working. Following accusations by Ukraine's Security Service (SBU), Russia denied responsibility, with the Kremlin spokesperson stating that "as expected, Ukraine continues blaming Russia for everything".

On February 22, the Red Bandits, a Russian cybercrime group, reported on Twitter that they hijacked dashcams of Ukrainian police officers. The group's post stated: "We've hijacked the @UkrainePolice Dashcams and have been watching them. If Ukraine does not do what #Russia wants we will escalate our attacks against Ukraine to involve panic scares. We will also consider distributing #ransomware in #UkraineRussiaCrisis". In another post published by the group on the same day, the Red Bandits claimed to have hacked Ukraine's internal government systems and secured information from confidential meetings between 2020 to 2022.

On February 23, the day before Russia's invasion, the websites of Ukraine's Ministry of Foreign Affairs, Security Service of Ukraine (SBU), Cabinet of Ministers, as well as banks suffered DDoS attacks. Ministries of infrastructure and education also experienced disruptions. Ukrainian soldiers likewise reported receiving text messages urging them to flee to avoid getting killed. The same day, cybersecurity experts at ESET and Symantec recorded a "wiper" malware attack used in Ukraine called HermeticWiper. These destructive attacks also leveraged two other components - HermeticWizard (spreads HermeticWiper across a local network) and HermeticRansom (ransomware written in Go).

HermeticWiper displayed a timestamp of 28 December 2021 suggesting that the attacks were prepared months in advance. According to ESET telemetry, the malware "was installed on hundreds of machines in the country". Symantec also reported that it uncovered evidence of HermeticWiper being used in Lithuania and Latvia. HermeticWiper was designed to target Windows devices and damage the MBR of the target systems, Despite its similarities with WhisperGate, IBM Security X-Force did not find code overlaps between the two. A joint Cybersecurity Advisory (CSA) from the US Cybersecurity and Infrastructure Security Agency (CISA) and Federal Bureau of Investigation (FBI) on February 26 provides information on WhisperGate and HermeticWiper malware as well as open-source indicators of compromise (IOCs).

On 24 February 2022, the first day of the invasion, MSTIC detected a new round of offensive malware directed at the Ukrainian government, dubbed FoxBlade. Ukraine's Computer Emergency Response Team (CERT-UA) was immediately notified of this and within three hours of detection, Microsoft's virus detection systems were updated to block the malware code. On the same day, ESET identified another wiper in Ukrainian government networks named IsaacWiper.

On 25 February 2022, Conti, a Russian-based ransomware group, pledged its "full support" of the Russian government. The group stated that "if anybody will decide to organize a cyberattack or any war activities against Russia, we [Conti] are going to use our all possible resources to strike back at the critical infrastructures of an enemy". Days after Conti made the announcement, its internal server containing the group's chat logs was hacked by a pro-Ukrainian group member revealing two years worth of internal data. Another group, Stormous, a self-described Arabic-speaking hacker group, also supported Russia by hacking into the Ministry of Foreign Affairs of Ukraine.

In a statement published on 28 February 2022, Microsoft noted the surge of cyber attacks against civilian targets in Ukraine. Microsoft president Brad Smith stated that the company was"especially concerned about recent cyberattacks on Ukrainian civilian digital targets, including the financial sector, agriculture sector, emergency response services, humanitarian aid efforts, and energy sector organizations and enterprises. These attacks on civilian targets raise serious concerns under the Geneva Convention, and we [Microsoft] have shared information with the Ukrainian government about each of them. We have also advised the Ukrainian government about recent cyber efforts to steal a wide range of data, including health, insurance, and transportation-related personally identifiable information (PII), as well as other government data sets".

Proofpoint, a US-based security firm, identified what is likely to be a nation-state sponsored phishing campaign targeting European government personnel involved in managing the logistics of refugees fleeing Ukraine. Using a possibly compromised Ukrainian armed service member's email account, the campaign distributed a malicious macro attachment which attempted to download a Lua-based malware dubbed SunSeed. While Proofpoint did not identify the perpetrator of the attack, it noted that it resembles a campaign previously carried out by Ghostwriter, also known as TA445 or UNC1151, which has previously worked to support the interests of Belarus.

Russia is allegedly using deep fake technology to promote its narratives in Ukraine. According to media reports, Russian 'troll farms' have been using AI technology to create fake bloggers on Facebook, Twitter and Instagram to promote misinformation about the war.

Cyber attacks targeting Russia and Belarus

On 25 February 2022, the Anonymous group hacked into the website of the Russian Ministry of Defense. They leaked a database containing phone numbers, email addresses and names of ministry employees. Reports also circulated online that "Cyber Troops of Ukraine" obtained access to a local Russian accounting and document management system containing personal information on a unit sent to Ukraine, including their passports, military IDs, personal details and credit card numbers. According to the information shared online, all the money from their cards will go toward the purchase of weapons for the Ukrainian armed forces.

Ukraine's Defense Ministry asked a Ukrainian cyber guerilla warfare group to deploy its capabilities against Russian railways and electrical grids. On 26 February 2022, Ukraine's Deputy Minister and Minister for Digital Transformation announced the creation of a volunteer cyber army. One of their key goals is to disrupt Russian infrastructure in an effort to make it impossible for them to transport weapons into Ukraine. Volunteer hacker groups use DDoS attacks against official Russian websites and create Telegram bots that block disinformation, allow people to report Russian troop locations, as well as publish instructions on assembling Molotov cocktails and providing basic first aid.

The “IT Army of Ukraine” is one of the largest communities of volunteers targeting Russia with cyber tools. Its channel on Telegram currently has over 307,500 subscriptions. Administrators of the channel post lists of targets in Ukrainian, Russian and English, which include business corporations (eg. Gazprom, Yandex), banks (eg. VTB, Sberbank), government agencies (eg. official website of the Russian president, Ministry of Defense), media agencies (eg. Ria, Kommersant), and YouTube channels of Russian media agencies (eg. Rossiya 24, TASS). The group also asked its followers to help disrupt the Moscow Exchange in an effort to lower the value of the Russian ruble, which reportedly only took five minutes. In addition to hacking, the channel posts personal information (eg. phone numbers) of famous Russian actors, influencers and political observers as well as Ukrainian celebrities supporting Russia. To raise awareness of what is happening in Ukraine, the channel asks its followers to spam Western media and NGOs with a call to “stop the genocide of Ukraine”.

On 27 February 2022, the IT Army of Ukraine expanded its scope to also include Belarus, a key Russian ally. As a result of an attack by the hacker group “Belarusian Cyber Partisans” (hacktivists fighting the Lukashenka regime), the Belarusian railway was switched to manual operation, while the Minsk and Orsha nodes were paralyzed.

On 28 February 2022, rumors circulated online surrounding Anonymous, alleging that they would empty the bank accounts of Russians and send the money to Ukraine. Anonymous published a statement on its official Twitter page challenging the rumors and emphasizing that “Anonymous will not attack the people but the government”. On the same day, it was reported that Anonymous took down more than 1,500 websites of Russian and Belarusian governments, state media outlets, banks and companies. While there is no concrete evidence that Anonymous generated these outcomes, many state websites of Russia and Belarus were inaccessible over the course of several days, including the websites of pro-Russian media.

On 1 March 2022, the main control center for Russia’s satellites was allegedly hacked by the Network Battalion 65’ (NB65) hacker group, which according to the alleged report resulted in the loss of control over a fleet of military spy satellites. The group’s message to Russia stated that they will not stop until Russia stops “dropping bombs, killing civilians and trying to invade”. However, Roscosmos, Russia’s state corporation responsible for space flights, cosmonautics programs, and aerospace research, denied any attack on its systems. The head of Roscosmos stated that “offlining the satellites of any country is actually a casus belli, a cause for war”.

Stories are circulating online urging regular people to participate in hacking operations against Russia. Avast Threat Lab researchers encouraged people to avoid such initiatives as the “simple user-friendly tools” that are being circulated online for hacking “can be a privacy and security risk for the person downloading it” and can further escalate the current situation.

On 8 March 2022, almost a dozen websites of Russian governmental agencies were hacked. Compromised websites featured anti-war images with the question ‘Why?’ written in the center. The affected agencies include the Federal Service for the Execution of Punishments; Antimonopoly service; Rosstat; Ministry of Culture; Ministry of Energy; Federal bailiff service; Agency for Youth Affairs; Federal Agency for Railway Transport; Agency for State Property Management; Federal Agency of Sea and River Transport; and the Federal Agency for Nationalities Affairs.

International response to the cyberwar

On 22 February 2022, the European Union announced the deployment of a cyber rapid-response team (CRRT) across Europe to support Ukraine's defense from cyber attacks. The team consists of eight to twelve experts from Lithuania, Croatia, Poland, Estonia, Romania and the Netherlands. An official stated that the team was "composed of different cyber-expertise, such as incident response, forensics, vulnerability assessment, to be able to react to a variety of scenarios".

On 1 March 2022, the US Senate unanimously approved a bipartisan package of cybersecurity bills, including legislation that would require critical infrastructure firms to report cyber incidents. Senate Homeland Security Committee Chair Gary Peters underlined that "this is especially important right now as we face increased risk of cyber attacks from Russia — and the cyber criminals that they harbor — in retaliation for our support for Ukraine". Notably, ahead of Russia's "operation" in Ukraine, the US Cybersecurity and Infrastructure Security Agency (CISA) issued a "shields up" alert.

On 4 March 2022, the NATO Cooperative Cyber Defense Centre of Excellence (CCDCOE) announced that Ukraine will become its "contributing participant". Through this cooperation, Ukraine will provide the Center with first-hand knowledge of cyber threat actors to support research, exercise and training. Previously in January 2022, Ukraine and the NATO Communications and Information (NCI) Agency signed a Memorandum of Agreement to deepen cooperation on cybersecurity and other projects in the digital domain.

On 11 March 2022, China reported that it had experienced continuous attacks since February. The Chinese National Computer Network Emergency Response Team / Coordination Center of China (CNCERT/CC) found that overseas groups took control of computers in the country to carry out cyber attacks against Russia, Ukraine and Belarus. Analysis showed that these attacks came from the US, while others were reportedly traced to Germany and the Netherlands.

About SecDev

SecDev is an agile research and innovation firm helping clients navigate digital-geopolitical, geospatial and geodigital risk. SecDev builds value through innovation in strategic foresight, data science and urban analytics. SecDev's team is fluent in technology, global in scope and results-oriented. SecDev empowers clients, such as national governments, technology companies and international organizations, to make informed choices that deliver value in the digital-urban age.

SecDev

Follow us on

LInkedin - https://www.linkedin.com/company/the-secdev-group
Facebook - https://www.facebook.com/secdev
Twitter - https://twitter.com/secdev


SecDevAnalytics