BRIEFING

European Parliament

Russia's war on Ukraine: Timeline of cyber-attacks

SUMMARY

Russia launched its war on Ukraine on 24 February 2022, but Russian cyber-attacks against Ukraine have persisted ever since Russia's illegal annexation of Crimea in 2014, intensifying just before the 2022 invasion. Over this period, Ukraine's public, energy, media, financial, business and non-profit sectors have suffered the most. Since 24 February, limited Russian cyber-attacks have undermined the distribution of medicines, food and relief supplies. Their impact has ranged from preventing access to basic services to data theft and disinformation, including through deep fake technology. Other malicious cyber-activity involves sending of phishing emails, distributed denial-of-service attacks, and use of data-wiper malware, backdoors, surveillance software and information stealers.

Organisations and governments around the world have not been indifferent to the hybrid risks thus posed. EU-, US- and NATO-led initiatives have been carried out with the aim of neutralising cyber-threats and protecting essential infrastructure. As part of these initiatives, the EU has activated its Cyber Rapid Response Teams (a project under Permanent Structured Cooperation (PESCO) in the area of security and defence policy), to support Ukraine's cyber-defence. Non-government and private players have supported Ukraine through various cyber-resilience activities. Since the beginning of the invasion, a significant number of counter-attacks have been launched by independent hackers, affecting the Russian state, security, banking and media systems.

The European Parliament has called for stepping up cybersecurity assistance to Ukraine and for making full use of the EU's cyber-sanctions regimes against individuals, entities and bodies responsible for or involved in the various cyber-attacks targeting Ukraine.

IN THIS BRIEFING

EPRS | European Parliamentary Research Service

Author: Jakub Przetacznik with Simona Tarpova
Members' Research Service

PE 733.549 – June 2022

EN

Background

Ukraine has been a permanent target of Russian cyber-attacks since at least 2014. Thousands of attacks occur every month, making Ukraine the 'perfect sandbox for those looking to test new cyber-weapons, tactics and tools' according to a *Politico* report. Since 24 February 2022, the attacks have had a limited scale, with the anticipated – but unsuccessful – attack against electricity grids taking place only during the second month of the war. Experts have speculated about the reason behind this 'conspicuous absence' of cyber-attacks. Explanations range from a high level of protection of Ukraine's information technology (IT) network to reliance of Russian military forces on Ukrainian IT infrastructure. While some experts note that Russian offensive cyber-capabilities may have been inflated, others suggest that Russia may simply be waiting for another opportune moment to launch massive attacks. A large-scale cyber-attack would have the potential to quickly spill over into other countries. On 21 March 2022, the US President, Joe Biden, urged US business leaders to strengthen their cyber-defence capacities, highlighting that Russia's use of its full spectrum of cyber capabilities poses a risk in and beyond Ukraine. The EU has taken a number of measures to support Ukraine's cyber-resilience and is working on improving its own.

Attacks since 24 February 2022

Since the beginning of Russia's war on Ukraine, initial examples of cyberwarfare have included: an attack on the communication systems of the *Kyiv Post* and the KA-SAT satellite network an hour before the invasion (24 February), an IssacWiper attack against government websites (25 February), a cyber-attack targeting a border control station with the aim of preventing refugees from entering Romania (25 February) and attacks on Ukraine's digital infrastructure, blocking access to financial services and energy (28 February). The operation targeting KA-SAT – resulting in communication outages for individuals and public and private Ukrainian entities – was condemned by the EU High Representative (HR) on 10 May. The HR described it as 'another example of Russia's continued pattern of irresponsible behaviour in cyberspace', adding that cyber-attacks targeting Ukraine 'could spill over into other countries and cause systemic effects putting the security of Europe's citizens at risk'. Cyber-attacks continued in March, with malware being launched against government and financial websites, as well as non-government, charity and aid organisations, in this case hindering the distribution of medicines, food and relief supplies. Other cases involve phishing attacks against citizens and government services, and attacks against telecommunication service providers, disrupting Ukrainian networks. On 14 March, the CaddyWiper malware infiltrated the systems of several Ukrainian organisations reportedly in both the government and the financial sectors. Two days later, a false message was aired on a Ukrainian TV channel, claiming that the Ukrainian President, Volodymyr Zelenskyy, had called on the population to surrender. A complementary deep-fake video of Zelenskyy was shared on a Telegram channel.

Cyber-attacks against Ukraine from the end of March include phishing emails targeting the government and the military (17 March) and various organisations (18 March), as well as the use of a LoadEdge backdoor for installing surveillance software (20 March). Cyber-assaults targeting Ukrtelecom and WordPress sites caused a connectivity collapse and restricted access to financial and government websites (28 March). On 30 March, the MarsStealer information stealer accessed the user credentials of Ukrainian citizens and organisations.

Similarly, in April, hackers extracted sensitive information and user credentials from the Ukrainian government (2 and 7 April) and media entities (7 April). They also seized citizens' banking and payment data with the help of a Trojan malware (14 April) and a fraudulent social media page survey (19 April). Other cyber-attacks sought to inflict societal harm. One such example included an attempt to hinder the activity of power stations and obstruct electricity flow to millions of people (8 April). The most recent attack succeeded in halting the work of the Ukrainian postal service while it was launching a series of war-related stamps (22 April).

In May, cyber-attacks were launched to complement military operations, targeting government websites, telecommunication services and infrastructure. For instance, an attack aimed at the Odesa City Council occurred at the time of a missile attack on the city's residential zones (7 May). Hackers also launched a distributed denial-of-service (DDoS) attack on some of Ukraine's telecom operators to filter and re-route online traffic to occupied territories (9 May).

Earlier attacks in 2022

Cyber-attacks soared at the beginning of 2022. For instance, on 13 January, Microsoft reported that malware had been detected targeting the Ukrainian government and several non-profit and IT organisations. The following day, 70 government websites, including that of the Cabinet of Ministers and the Ministries of Defence, Foreign Affairs, Education and Science, ended up being temporarily controlled by hackers. The Ukrainian Ministry of Digital Transformation held Russia responsible.

In mid-February, a DDoS attack knocked out the websites of several government departments, banks and radio stations for a few hours. Several countries accused Russia of launching the attack to wreak panic and confusion among Ukrainians. The same websites, including that of the Cabinet of Ministers and several ministries, were targeted again on 23 February. Additionally, the HermeticWiper data-wiping malware was launched against 100 organisations from the financial, IT and aviation sectors.

Attacks in the 2016-2021 period

Between 2016 and 2021, cyber-attacks on Ukraine had already intensified. The most notable one involved the launch of the NotPetya malware – considered history's most destructive cyber-attack – through accounting software in June 2017. NotPetya hit the Chornobyl nuclear power plant and close to 13 000 devices used by public institutions, banks, postal services, newspapers, transport infrastructure and businesses. The computer drives were destroyed, disabling data restoration after the virus encryption. The malware had a global impact, affecting 65 countries and about 50 000 systems, including European and US companies FedEx, Maersk and Merck, and inflicting a loss of over US$10 billion.

Two major attempted cyber-attacks occurred in 2018 and 2021. The former was aimed at the Auly chlorine distillation station, which operates in 23 Ukrainian provinces, while the latter targeted the Ukrainian security service websites. An attack against the electronic interaction system used by the government executive bodies failed but succeeded in inflicting damage to the system.

Attacks in 2014 and 2015

On 13 March 2014, three days before the referendum on the status of Crimea, Russia launched an eight-minute-long DDoS cyber-attack aimed at destabilising Ukrainian computer networks and communications as a way to divert public attention from the presence of Russian troops in Crimea. In May 2014, prior to the Ukrainian presidential elections, a pro-Russian hacktivist group carried out a series of cyber-attacks to manipulate the vote. The CyberBerkut hackers invaded the network and deleted files in an attempt to change the election results by targeting the Central Election Commission. The attack failed, as the malware was removed 40 minutes before the election (25 May). However, the hackers managed to delay the election count.

In the following couple of years, Ukrainian authorities ascribed two cyber-attacks on power grids to Russia. On 23 December 2015, another DDoS attack affected call centres and the network of three energy distribution companies. As a result, over 230 000 consumers in western Ukraine experienced power outages ranging from one to six hours. Moreover, the allegedly Russian state-sponsored Sandworm Team succeeded in hindering the systems of 16 electrical substations. A similar cyber-attack occurred in 2016. Disruptions in a Kyiv substation resulted in a one-hour power blackout, but the attempt failed to completely disable the equipment.

Figure 1 –Timeline of cyber-attacks on Ukraine

Source: Data compiled by EPRS; Graphic by Lucille Killmayer.

Counter-cyber-attacks

Although Ukraine has limited counter-attack capacities, it has endeavoured to boost its cyber-defence with external assistance. The government has gathered international volunteers to form an IT army. In retaliation to Russian attacks, the IT team set up by the minister of digital transformation has launched several DDoS and wiper attacks. The former disrupts the functioning of servers by artificially creating traffic, while the latter entails data deletion. Targets include Russia's government, media systems, financial institutions, defence facilities, power grids and railways.

As part of counter-cyber-attacks, independent hackers from all over the world have stolen and exposed Russian government and financial data, including emails, information on banking activities, energy production and propaganda campaigns, and the details of troops and Federal Security Service (FSB) agents. This sensitive information is then reportedly shared with global activists as a way to penalise Russia for its crimes in Ukraine. A secondary effect of the hackers' recent activities is their success in inflicting chaos on Russian cyber-systems and shattering the perception of Russia's impregnable cyber-defence.

EU and international response

The EU has supported Ukraine in countering cyber-attacks by launching the EU–Ukraine cyber-dialogue (June 2021), strengthening the operational capacity of the country's telecommunications services, and combating disinformation. Additionally, following a request from the Ukrainian government, the EU activated PESCO's Cyber Rapid Response Teams (February 2022) for the first time in an operational context. The cybersecurity experts will provide assistance on threat detection, recognition and mitigation. Earlier, the EU had imposed the first-ever sanctions against the masterminds of cyber-attacks, including NotPetya, in July 2020. The recently endorsed Strategic Compass aims to strengthen the cyber-resilience of the EU (inter alia by proposing a new cyber-resilience act and further strengthening the Cyber Diplomacy Toolbox), but also that of the EU's eastern partners through cooperation on countering hybrid and cyber threats, and disinformation.

In February 2022, a US Cyber Command team assisted the Cyber Rapid Response Teams in searching for active threats. For its part, since 2017, the US has contributed US$40 million to developing Ukraine's IT sector. NATO allies have also invested in Ukraine's cyber-defence through information-sharing and support on the ground. In March 2022, Ukraine became a contributing participant in NATO's Cooperative Cyber Defence Centre of Excellence. Furthermore, private players, such as Microsoft, Amazon and Google are assisting Ukraine in detecting and countering cyber-attacks during the invasion. The European Centre of Excellence for Countering Hybrid Threats has also strengthened its cooperation with Ukraine since the beginning of the war, by observing the context and organising exercises.

European Parliament position

In its resolution of 1 March 2022, the Parliament called for immediate and full implementation of all decisions that would increase the EU's contribution to strengthening Ukraine's defence capacities, including cybersecurity. Moreover, the Parliament urged the EU, NATO and other like-minded partners to intensify their cybersecurity assistance to Ukraine. MEPs called for the EU cyber-sanctions regime to be fully used against individuals, entities and bodies responsible for or involved in cyber-attacks against Ukraine.

In the past, the Parliament has repeatedly insisted that the EU should provide Ukraine with assistance in countering hybrid threats (e.g. cyber-attacks and disinformation); Parliament has also supported greater investment in Ukraine's cybersecurity. The Parliament's recommendation of 8 June 2022 called for swift implementation of the Strategic Compass, including its cyber aspects; it furthermore recommended that the Council and the High Representative of the Union for Foreign Affairs and Security Policy/Vice-President of the Commission make full use of the EU cyber-sanctions

regimes against individuals, entities and bodies responsible for or involved in the various cyber-attacks targeting Ukraine.

The Parliament resolution of 8 June 2022 on security in the Eastern Partnership (EaP) area and the role of the common security and defence policy contains several specific suggestions. The resolution recognises that the EU's strategic interest can encompass inclusion of associated EaP countries (countries that have association agreements with the EU, namely Ukraine, Moldova and Georgia) in individual PESCO projects, especially in the areas of hybrid threats and cybersecurity. The resolution called for exploring options to foster the cyber-capabilities of EaP countries, and proposed to launch civilian cyber missions. Regarding the European Union Advisory Mission (EUAM) in Ukraine, the resolution called for the extension of its mandate to cover combating hybrid threats, strategic communication, digital technology and cybersecurity.

MAIN REFERENCES

A Strategic Compass for Security and Defence, EEAS, March 2022.

Activation of first capability developed under PESCO points to strength of cooperation in cyber defence, EDA, February 2022.

Antoniuk, D., 'DDoS attacks hit Ukrainian government websites', *The Record*, February 2022.

Attribution to Russia of malicious cyber activity against Ukraine, Australian government, February 2022.

Brumfield, C., Russia-linked cyber-attacks on Ukraine: A timeline, CSO, April 2022.

Cerulus, L., 'How Ukraine became a test bed for cyberweaponry', *Politico*, February 2019.

Cerulus, L., 'Ukraine is getting pummeled with cyber-attacks. What's the West to do?', *Politico*, February 2022.

Cimpanu, C., 'Hackers deface Ukrainian government websites', *The Record*, January 2022.

Cimpanu, C., Ukraine reports cyber-attack on government document management system, Zdnet, February 2021.

Clayton, M., 'Russia Hammers Ukraine With Massive Cyber-Attack', *Business Insider*, March 2014.

'Cyber-attacks on Ukraine are conspicuous by their absence', *Politico*, March 2022.

Deputy Secretary General stresses NATO will continue to increase Ukraine's cyber defences, NATO, January 2022.

EU imposes the first ever sanctions against cyber-attacks, Council of the European Union, July 2020.

Fendorf, K. and Miller, J., Tracking Cyber Operations and Actors in the Russia-Ukraine War, Council on Foreign Relations, March 2022.

Harding, L., 'Ukraine hit by 'massive' cyber-attack on government websites', *The Guardian*, January 2022.

Hern, A., 'Ukrainian blackout caused by hackers that attacked media company, researchers say', *The Guardian*, January 2016.

Holland, Steve. and Pearson J., US, UK: Russia responsible for cyber-attack against Ukrainian banks, Reuters, February 2022.

Hybrid CoE continues to work to support European security and Ukraine, Hybrid CoE, March 2022.

Ishak, N., Is Russia holding back from cyberwar?, Vox, March 2022.

Kagubare, I., 'US, EU cyber investments in Ukraine pay off amid war', *The Hill*, March 2022.

Madiega, T., Russia's war on Ukraine: The digital dimension, EPRS, March 2022.

Madnick, S., 'What Russia's Ongoing Cyber-attacks in Ukraine Suggest About the Future of Cyber Warfare', *Harvard Business Review*, March 2022.

Menn, J., 'Hacking Russia was off-limits. The Ukraine war made it a free-for-all', *Washington Post*, May 2022.

Miller, M., 'Despite years of preparation, Ukraine's electric grid still an easy target for Russian hackers', *Politico*, February 2022.

NotPetya, CyberLaw, May 2019.

NotPetya, Five Facts to Know About History's Most Destructive Cyber-attack, HYPR, June 2017.

Resolution of 1 March 2022 on the Russian aggression against Ukraine (2022/2564(RSP)), European Parliament, 1 March 2022.

Resolution of 11 February 2021 on the implementation of the EU Association Agreement with Ukraine (2019/2202(INI)), European Parliament, 11 February 2022.

Scroxton, A., 'Ukraine joins Nato cyber knowledge hub', *Computer Weekly*, March 2022.

UK assesses Russian involvement in cyber attacks on Ukraine, Foreign, Commonwealth & Development Office and National Cyber Security Centre, United Kingdom, February 2022.

Ukraine accuses Russian networks of new massive cyber attacks, Reuters, February 2022.

'Ukraine power cut 'was cyber-attack'', BBC, January 2017.

Ukraine: Timeline of Cyber-attacks on critical infrastructure and civilian objects, CyberPeace Institute, April 2022.

Vazquez, M., Judd D., Lyngaas S. and Cohen, Z., 'Biden warns business leaders to prepare for Russian cyber attacks', CNN Politics, March 2022.

What is a DDoS attack?, Cloud Flare.

Wiper Attacks, Firewalls Security Blog.

Wolff, J., 'Why Russia Hasn't Launched Major Cyber Attacks Since the Invasion of Ukraine', *Time*, March 2022.

DISCLAIMER AND COPYRIGHT

eprs@ep.europa.eu (contact)

www.eprs.ep.parl.union.eu (intranet)

www.europarl.europa.eu/thinktank (internet)

http://epthinktank.eu (blog)