NOTRE EUROPE
Jacques Delors Institute
Penser l'Europe • Thinking Europe • Europa denken

```
 function () {
pen()) return;
moveClass(_json.ClassOpen);
tBtnOpen.Show();

 plein écran
reenEnabled = function () {
dClass(_json.ClassFullscreen);

e plein écran
reenDisabled = function () {
moveClass(_json.ClassFullscreen);

e la viewport est ouverte
 function () {
$elm.hasClass(_json.ClassOpen);

après la récupération du HTML
 via ajax
 (response, textStatus) {
```

© Photo by Sigmund on Unsplash

Cyberattacks in Russia's hybrid war against Ukraine

and its ramifications for Europe

EUROPE IN THE WORLD

POLICY PAPER N°281
SEPTEMBER 2022

#ukraine
#defence

Arnault Barichella
Associate
Research Fellow in
Cybersecurity and
Digital Technologies

• Executive summary

- Following the annexation of Crimea and the outbreak of military tensions in the Donbas in 2014, a decade-long cyber confrontation has been ongoing between Russia, Ukraine and the West, with Russian-backed hackers unleashing some of the most destructive cyberattacks in history. There was widespread apprehension that the Russian invasion of Ukraine in February 2022 would lead to a new wave of major cyberattacks. Although cybersecurity has certainly played a key role in the Ukraine war, this has not unfolded in the way many had expected.
- From an internal perspective, while Russian hackers launched multiple cyber assaults against Ukraine since February, these have mostly consisted in medium to low-scale attacks involving spying, psychological disruption and 'hybrid warfare', which combines targeted cyberattacks with kinetic military strikes on the ground. From an external perspective, cyberattacks on Ukraine have resulted in limited spillover into Europe. Instead, Moscow has amplified its cyber espionage and disinformation campaigns against the West, attempting to sow internal disunity.
- Remarkable cyber resilience on the part of Ukraine has been a decisive factor, with Kyiv learning from past mistakes. Europe and the West have provided extensive support to Ukraine through the transfer of IT equipment, software and the provision of training/expertise. Real-time cyber intervention from European and US cyber agencies, along with private sector assistance, have been crucial. Due to the initial expectation of a short war, Moscow poorly prepared its cyber offen-

sive against Ukraine; crippling Western economic sanctions, together with a brain drain of Russian IT experts, have also played a role. Fear of cyber retaliation from NATO or of major cyberattacks inadvertently leading to direct military confrontation, have led to a 'cyber-MAD' or 'cyber Cold War' stand-off between Russia and the West, at least for the time being.

- Yet, **the danger of cyber escalation should not be underestimated, especially if Russian military operations on the ground are unsuccessful and the Kremlin deems itself cornered.** The risk of misunderstanding is exacerbated by the involvement of a global coalition of hackers led by 'Anonymous', which launched a sustained campaign of cyberattacks against Russia. Hence, Europe must not let its guard down and should accelerate cyber assistance to Ukraine through existing tools like 'Cyber Rapid Response Teams', and by developing new ones such as civilian cyber operations. The EU also needs to do more to tackle disinformation while reinforcing its policies and legislation on cybersecurity, especially in terms of addressing the issue of weak links stemming from differentiated norms across Member States.

Résumé

- Suite à l'annexion de la Crimée et le début des tensions militaires dans le Donbass en 2014, la Russie, l'Ukraine et l'Occident s'affrontent dans un cyber-conflit continu depuis presque dix ans. Des pirates informatiques, soutenus par le Kremlin, ont déclenché des cyber-attaques parmi les plus destructrices de l'histoire au cours des dernières années. Ainsi, l'invasion russe de l'Ukraine en février 2022 a suscité les craintes d'une nouvelle vague de cyber-attaques d'envergure. Même si la cybersécurité a indéniablement joué un rôle clé dans la guerre en Ukraine, cela ne s'est pas produit de la manière anticipée.
- D'un point de vue interne, alors que la Russie lance depuis février de multiples cyber-attaques contre l'Ukraine, celles-ci ont principalement été de moyenne échelle, comprenant l'espionnage, des attaques symboliques et psychologiques, ainsi qu'une forme de « guerre hybride » combinant des cyber-attaques ciblées avec des frappes militaires cinétiques. D'un point de vue externe, la propagation vers l'Europe des cyber-attaques visant Ukraine a été limitée. Moscou a en revanche accru son cyber-espionnage et ses campagnes de désinformation contre l'Occident, cherchant à semer la désunion interne.
- Une cyber-résilience remarquable de la part de l'Ukraine a été un facteur décisif, Kiev ayant tiré les leçons de ses erreurs passées. L'Europe et l'Occident ont fourni un soutien important à l'Ukraine via le transfert de matériel informatique et de logiciels, ainsi que par le biais de formations et la provision d'expertise. Des interventions en temps réel par les agences cyber européennes et américaines, associées à l'aide précieuse du secteur privé, ont été cruciales. S'attendant initialement à une guerre courte, Moscou avait mal préparé sa cyber-offensive contre l'Ukraine ; les sanctions économiques occidentales sévères, associées à une fuite de cerveaux d'experts informatiques russes, ont également joué un rôle important. La crainte d'une cyber-riposte massive de l'OTAN ou de cyber-attaques menant par inadvertance à une confrontation militaire directe, ont conduit à une situation comparable à celle d'une « cyber-guerre froide » entre la Russie et l'Occident, du moins pour l'instant.
- Cependant, **il ne faudrait pas sous-estimer le danger d'une escalade dans le domaine cyber, surtout si les opérations militaires russes sur le terrain tournent mal et que le Kremlin s'estime pris au piège**. Le risque de malentendu est exacerbé par l'intervention d'une coalition internationale de pirates informatiques menée par « Anonymous », qui a lancé une redoutable campagne de cyber-attaques contre la Russie. L'Europe ne doit donc pas baisser la garde et devrait renforcer son assistance à l'Ukraine dans ce domaine en employant des

politiques existantes telles que les « cyber-équipes d'intervention rapide », et en développant de nouveaux outils tels que des opérations civiles de cybersécurité. L'UE doit également agir davantage pour lutter contre la désinformation, tout en renforçant ses politiques et sa législation dans ce domaine, notamment pour faire face au problème des maillons faibles en lien avec les normes cyber différenciées en vigueur au sein des États membres.

Introduction

The Russian military invasion of Ukraine on the 24th of February 2022 represents one of the significant geopolitical crises since the Second World War. Although Russia began massing troops on its Western border in March 2021, few anticipated the magnitude of the subsequent assault, which rapidly escalated into a full-scale military invasion with an attempt by Russian forces to annex Ukraine and topple the democratically elected regime in Kyiv. The conflict also resulted in Europe's largest refugee crisis since 1945, with over seven million people forced to flee the country due to the war and more than eight million people being displaced internally.[1] The war in Ukraine also led to a complete breakdown in relations between NATO and Russia and perhaps the closest the world has come to nuclear war since the Cuban missile crisis in 1962, with both sides openly threatening to retaliate with nuclear weapons in response to perceived aggression.[2] Likewise, the economic repercussions of the Ukraine conflict have been substantial, with Western countries (the US, the EU/EEA, UK, Canada, Australia/New Zealand along with Japan) imposing the most drastic and far-reaching set of international sanctions ever enacted in history against another country, in this case the Russian federation. The latter retaliated in kind, including by significantly reducing fossil fuel exports to Western countries and especially to Europe, which had up until then relied on Russia as its main supplier of oil and gas. All of this has led to a major global economic downturn and inflation crisis, with a sharp rise in energy prices around the world.

Given the magnitude of such events, it is not surprising that the cybersecurity dimension of the war in Ukraine has been somewhat overlooked in Western media. This paper will aim to highlight the different ways in which cybersecurity represents a vital element of the Ukraine war, even though the cyber dimension has not unfolded in the way many had anticipated. Instead of large-scale cyberattacks successfully knocking out wide sections of Ukrainian infrastructure, the conflict has initiated a full 'hybrid' war. The latter has involved psychological disruption, persistent cyber espionage and sustained medium to low-scale cyberattacks in support of and often in tandem with conventional military operations on the ground. From an external perspective, only limited spillover has resulted from hackings in Ukraine, whilst Russia has not launched major cyberattacks against NATO countries in retaliation for sanctions and support to Ukraine, only low-scale direct attacks. Moscow has opted instead to amplify its espionage and disinformation warfare against Europe and the West more generally, which has started to yield some results. Nevertheless, the risk of escalation and of the Ukraine conflict developing into a highly destructive cyber world war is genuine and should not be underestimated, since both NATO and Russia possess the requisite cyberweapons and have threatened to use them on multiple occasions. As will be examined in the following sections, much will depend on how the military situation evolves in Ukraine over the next few months, and whether Moscow senses that it risks losing the upper hand in the war.

[1] UNHCR, *Operational Data Portal: Ukraine Refugee Situation.* See: https://data.unhcr.org/en/situations/ukraine

[2] The nuclear aspect also includes ongoing concerns over the security of the *Zaporizhzhia* nuclear power plant in southeastern Ukraine, the largest of its kind in Europe, which has come under shelling and currently finds itself in the middle of a battlefield.

I . Background on the role of cybersecurity in relations between Russia, Ukraine and Europe over the last decade

I BACKGROUND ON THE CYBERSECURITY DIMENSION OF THE RUSSO-UKRAINIAN CONFLICT OVER THE LAST DECADE

Geopolitical dynamics are now widely believed to be one of the main factors behind a global rise in cyberattacks over the last few years.[3] Cyber operations have the advantage of offering the assailant at least partial concealment, since attribution remains challenging due to frequent reliance on false flags, for example. This has led a number of influential countries to increasingly rely on cyberwarfare to achieve geopolitical objectives by appropriating large quantities of sensitive information or by causing major damage to infrastructure, without openly revealing themselves. Amongst these, Russia is widely believed to be one of the most active nations in the world within the cyber realm, with a significant number of global cyberattacks over the last few years suspected to have originated from hacker groups affiliated to the Kremlin, or directly from Russian military and security entities.[4] In this regard, Ukraine has been one of the primary targets of Russian-backed cyberattacks over the last decade, to the extent that the country is often considered to be Moscow's 'playground' for testing and developing new cyberweapons.[5]

Russia was one of the first nations to launch a cyberattack against another country for geopolitical reasons when it targeted Ukraine with the *Uroburos* Trojan malware[6], perhaps as early as 2008. While cybersecurity has been a characteristic aspect of tensions between Russia and Ukraine for a long time, it was not until 2013 that Russia notably increased the pace and sophistication of its cyberattacks. This was in response to the 'Euromaidan' protests which erupted in November 2013, followed by the 'Revolution of Dignity' that took place in February 2014. The latter led to the downfall of pro-Russian President Viktor Yanukovych and the initial outbreak of the Russo-Ukrainian War, with Moscow annexing the Crimean Peninsula in the south and Russian troops entering the Donbas region in the east to support the two breakaway "states" of Luhansk and Donetsk. In order to destabilize Ukraine in support of Russian military interventions, several notable cyberattacks were carried out. 'Operation Armageddon' led to widespread cyber espionage on Ukrainian government, judicial and military institutions. The latter was followed by 'Operation Snake', which involved a multitude of so-called 'distributed denial of service' (DDoS)[7] attacks targeting governmental websites, mass media and communications, possibly in an attempt to divert attention or cause chaos during troop operations in Crimea. Just a few months later in May 2014, pro-Russian hackers tried to manipulate the vote of the Ukrainian Presidential election by launching cyberattacks on the Central Election Commission; although this attack failed to alter the result, it still succeeded in delaying the voting count.

[3] Barichella A., *European Cybersecurity and Data Privacy: Threats and Prospects*, Policy Brief – Jacques Delors Institute, March 2022.

[4] *Ibid.* This includes the Main Directorate of the General Staff of the Russian Armed Forces (still often referred to by its former acronym GRU), the Foreign Intelligence Service (SFR), as well as the Federal Security Service (FSB). Hacking groups with ties to these Russian State entities include 'Fancy Bear', 'Cozy Bear', 'Sandworm' or 'Killnet' amongst others, who either directly operate under instructions and funding from the Kremlin, or are indirectly sponsored and encouraged by the latter.

[5] Barichella A., *Cybersecurity in the Energy Sector: A Comparative Analysis between Europe and the United States*, Études de l'Ifri, February 2018.

[6] Malware can be defined as software that is specifically designed to disrupt, damage, or gain unauthorized access to a computer system.

[7] A 'distributed denial-of-service' or DDoS attack involves an attempt to disrupt a computer system by overwhelming it with a flood of massive requests and Internet traffic until collapse.

Following the integration of Crimea into Russia in March 2014[8], along with the initial outbreak of military conflict in the Donbas, Moscow amplified its cyberattacks against Ukraine in a decade-long attempt to destabilize the country. Hence, the cyber dimension of the Russo-Ukrainian war began in 2013-14 and has continued through the current conflict, in parallel with protracted military confrontation in the Donbas. During this period, Russia launched several of the most devastating cyberattacks in history on Ukrainian critical infrastructure. Prominent examples include the *Black Energy* virus in December 2015, which succeeded in shutting down thirty Ukrainian electrical stations, cutting off the power supply for over 200,000 people in eight different provinces for several hours. This was followed by another similar cyberattack the following year in December 2016, with disruptions to a power utility in Kyiv leading to a one-hour blackout (even though this time, hackers were unable to completely disable the utilities). The latter set the stage for a devastating series of cyberattacks in 2017, beginning with the *XData virus*, which paved the way for one of the most destructive malwares ever unleashed (and certainly the most destructive at the time) in June that year. Known as the *NotPetya* virus, this malware infected more than 13,000 devices and nearly 30% of all computer systems across Ukraine including public institutions, the postal system, banks and businesses, media and communications, as well as transport and energy infrastructure (like the Chornobyl nuclear plant), wiping out computer drives and disabling data restoration.[9] It is notable that *NotPetya* was not limited to one country but spread globally, affecting in total sixty-five different countries and approximately 50,000 computer systems worldwide, including many Western firms such as the French group Saint-Gobin, the Danish transporter Maersk or the US services firm FedEX, with total losses amounting to more than $10 billion. Subsequently, Russia launched several other notable cyberattacks in the years leading up to the 2022 invasion (albeit on a lesser scale), including one in July 2018 aimed at the *Auly* chlorine distillation station serving 23 different Ukrainian provinces.

BACKGROUND ABOUT THE CYBERSECURITY DIMENSION IN RELATIONS BETWEEN RUSSIA AND EUROPEAN/NATO COUNTRIES OVER THE LAST DECADE

The *NotPetya* virus highlighted the extent to which cyberattacks, even when they target a particular country, can subsequently propagate internationally due to the globalization of digital technologies and economic interdependence of transnational businesses. Following the first imposition of economic sanctions on Russia by the EU and the US in 2014 for its annexation of Crimea and role in the outbreak of the Donbas war, relations between Moscow and the West steadily declined and reached a low point several years before the full-scale invasion of 2022. Thus, even though attribution remains problematic for reasons discussed above, Russian security entities and/or pro-Moscow hackers are the prime suspects behind a wave of major cyberattacks that have directly targeted European and Western nations. This includes not only former Soviet countries like Poland or the Baltic states, but also Germany, France, the UK and the US.

Similarly to Ukraine, cyberattacks launched by Russia against the West have been ongoing since at least 2014, if not before. In 2007 for instance, due to a diplomatic dispute with Moscow over a Soviet war memorial, Estonia was hit by a series of devastating cyberattacks that brought down the websites of governmental, media

[8] It should be noted that following the annexation, Crimea's fiber optic cables were altered to cut off connection between the peninsula and mainland Ukraine, redirecting all online communications towards Russia. This reduced the possibility for retaliatory cyberattacks from Kyiv or the West.

[9] *NotPetya* represents a prominent example of a so-called 'wiper' type of malware, which aims to wipe out all of the data on the hard drive of the infected computer system, thus preventing data restoration.

and financial institutions through DDoS attacks.[10] More recently, a three-year long disinformation campaign operating via social media platforms like Facebook was uncovered in Poland in early 2019; a stream of fake news in support of three pro-Russian Polish politicians reached an audience of up to 4.5 million people.

Likewise, German security officials have accused Russian-backed groups of hacking into the files of a Parliamentary Committee investigating the NSA spying affair in 2015. This was followed by a series of cyberespionage and data breaches in 2016 and 2017 against various German political entities, along with disinformation campaigns relying on social media platforms, possibly in an attempt to influence the 2017 German federal elections. Moreover, the French broadcasting service TV5Monde was hit by a major cyberattack in 2015 which destroyed computer systems and took off the air all of its twelve channels; French authorities subsequently found that the Russian-backed group 'Fancy Bear' was probably behind the hacking. Just before the French Presidential election in May 2017, the computer systems of Emmanuel Macron's political campaign were also hacked into, with over 20,000 emails stolen and then dumped on an anonymous file-sharing site, in an effort to destabilize his campaign. Once more, ensuing investigations found links with the 'Fancy Bear' hacker group.

Despite the difficulties in attributing cyberattacks, there are also strong suspicions of active Russian-backed disinformation efforts during the campaign leading to the UK's Referendum on EU membership in 2016, relying on social media platforms to promote pro-Brexit views. In fact, the UK government's voter registration website collapsed in June that year less than two hours ahead of the scheduled registration deadline, possibly due to a DDoS attack which may have had links to Russian-backed hackers.[11] In this regard, there is a notable parallel with the hacking and disinformation campaigns that marred the 2016 US Presidential election. Examples of interference involve emails stolen from the Democratic National Committee, including from Hillary Clinton and her campaign chairman John Podesta, which had a notable media impact at the time and might have contributed to influencing the outcome of the election. This was accompanied by a sustained disinformation operation, where Russian-backed groups are suspected to have relied once more on various social media platforms to promote anti-Hillary Clinton and pro-Trump slogans over several months.

In addition to this type of disinformation cyberwarfare, it should be noted that the US and Europe have also been exposed to a wave of direct cyberattacks over the last few years. One prominent example is the Colonial Pipeline ransomware attack of May 2021, which hit the largest American oil pipeline and led to a complete halt of all its operations, resulting in major fuel shortages and a regional declaration of emergency for 17 US states plus Washington, D. C. This represented the largest cyberattack on energy infrastructure in US history; the FBI traced its origin to the 'DarkSide' hacker group with ties to Russia.[12] Another significant cyberattack was the

[10] In response to this wave of cyberattacks, the Estonian government launched far-reaching reforms to enhance cybersecurity training and defenses across the country, which have led Estonia to become one of the leading IT nations in the world. This provided an example that Ukraine would subsequently follow, as will be examined below.

[11] Subsequent investigations have not been conclusive however, with some reports suggesting that the website could also have collapsed due to a spike in user login just before the deadline for voter registration, which was extended as a result.

[12] A ransomware cyberattack is a type of malware which involves a hacker threatening to block access to a service or release confidential data/information unless a ransom is paid; in this case, the Colonial Pipeline Company agreed to pay a large ransom in bitcoin in exchange for the restoration of computer systems. While the 'DarkSide' hacker group is believed to have close ties with Russia and is probably even based there, it may not take direct orders from the Kremlin.

Solar Winds hacking, which affected thousands of public and private organizations globally but appears to have especially targeted entities in the US and Europe. This includes a variety of US federal departments (Commerce, Defense, State, Treasury, Homeland Security, Labor, Energy, Justice, Health and Agriculture amongst others), as well as NATO institutions, the European Parliament, and a number of national governments in Europe such as the UK and Spain. The *Solar Winds* cyberattack led to significant data breaches and is believed to be one of the worst cyber-espionage operations ever to target the US and Europe due to the sensitivity of information stolen, the high profile of targeted institutions, as well as the prolonged time period (eight to nine months) before it was finally uncovered in December 2020. Subsequent investigations have revealed that a combination of Russian security/military agencies, together with several groups of hackers with close ties to the Kremlin, were most likely behind the attack,[13] leading US Democratic Senator Richard J. Durbin to claim at the time that the cyberattack was potentially equivalent to a declaration of war.[14]

II • How the cyber dimension of the current Ukraine war unfolded differently than expected

THE INTERNAL CYBER DIMENSION OF THE UKRAINE WAR: SUSTAINED MEDIUM TO LOW-SCALE CYBERATTACKS, PSYCHOLOGICAL WARFARE, PERSISTENT CYBER ESPIONAGE AND 'HYBRID' MILITARY OPERATIONS

For reasons discussed in the previous section, it is clear that cybersecurity has been at the forefront of conflict between Russia and Ukraine, as well as the resulting wider confrontation between Moscow and the West, at least since the annexation of Crimea and the initial outbreak of military hostilities in the Donbas in 2014. Major Russian cyberattacks continued up until the launching of a full-scale invasion of Ukraine in February 2022. Consequently, a number of experts, politicians and defense officials anticipated that the war would be characterized by large-scale cyberattacks launched by both sides, including against governmental and military entities, along with critical infrastructure.[15] As explained in the introduction, however, while cybersecurity has played a key role since the Russian invasion began last February, this has not unfolded in the way that many had predicted, or indeed in the manner of previous major Russian cyberattacks over the past few years. Unsurprisingly, Moscow amplified its cyberattacks against Ukraine in the months leading to the invasion as it was building up its troops along the border, in an attempt to destabilize the country. Examples include attempted hacks in early to mid-2021 against Ukrainian security websites and the computer systems relied upon by senior governmental entities. The rate of cyberattacks accelerated at the beginning of 2022 just before the invasion. For instance, malware known as *WhisperGate* was launched in mid-January targeting 70 governmental websites that were temporarily disabled, including the Cabinet of Ministers and the Ministries of Foreign Affairs, Defense, Science and Education. Likewise in mid-February, a DDoS attack again shut down the websites of a number of governmental departments, radio stations and banks during a couple of hours.

[13] This includes the FSB, SVR, along with hacker groups such as 'Cozy Bear' and 'Berserk Bear' with close ties to Russian State entities.

[14] Gould J., *No. 2 Senate Democrat decries alleged Russian hack as 'virtual invasion'*, C4ISRNet – 17 December 2020. See: https://www.c4isrnet.com/congress/2020/12/17/no-2-senate-democrat-russia-hack-a-virtual-invasion/

[15] This is especially the case since Russia's latest military doctrine places cybersecurity as a top priority, and openly refers to the possibility of launching offensive cyberattacks to defend vital strategic interests.

As had been expected, the Russian military ground invasion begun on 24 February 2022 was accompanied by the unleashing of several larger and more destructive cyberattacks, mostly involving 'wiper' type malware. The day before the invasion, the *Hermetic Wiper* virus destroyed around 300 computer systems across the country, targeting over one hundred different governmental, financial, energy, aviation and IT organizations. This was followed the day after by what has probably been Russia's most successful cyberattack since the invasion begun. In order to support the launching of military operations on the ground, hackers targeted the satellite company Viasat with destructive malware, which resulted in the disabling of tens of thousands of modems linked to the Viasat Inc's KA-SAT satellite. The cyberattack succeeded in disrupting communications across Ukraine, with a notable impact on the country's governmental and military communications in the early stages of the war (there was also a spillover into Europe – see next section). On February 25, another destructive wiper virus known as the *Isaac Wiper* was launched against Ukrainian governmental computer networks, followed in mid-March by the *Caddy Wiper* malware which infiltrated the systems of several financial and governmental organizations. Moreover, on March 28, cyberattacks targeted 'Ukrtelecom', one of Ukraine's largest telecom providers, lowering connectivity across the country to 13% below pre-war levels. On the same day, a series of DDoS attacks, relying on WordPress sites, simultaneously targeted 10 websites from governmental agencies, financial entities and think tanks.

The aforementioned cyberattacks should not be underestimated and certainly played a role in terms of disrupting Ukraine, helping Russian troops to progress on the ground. However, it is striking to what extent they are smaller in scale and have clearly had a more limited impact compared to some of the previous Russian cyberattacks, especially the *Black Energy* or *NotPetya* viruses for example (see first section). It should be noted that several attempts were made by Moscow-backed hackers to unleash more destructive malware on an equivalent scale, for instance on April 8 when several Ukrainian power stations were targeted, with the objective of cutting off the supply of electricity for millions of people. While the aim was undoubtedly to repeat similar damage as with the *Black Energy* virus of 2015,[16] the cyberattack ended in failure. The same is also true of several other attempts made by Russian hacker groups to launch cyberattacks on a larger scale over the last few months, discussed below. It is important to emphasize that this forced the Russian military to rethink its cyber strategy in the wake of these unexpected setbacks. Instead of launching a wave of large-scale and destructive cyberattacks, Moscow seems to have adapted its approach by focusing instead on sustained medium to low-scale cyber harassment operations aimed not only at governmental or military institutions, but also at financial, media and communication entities, as well as all other aspects of Ukrainian civil society including universities, NGOs and charity/aid organizations.

One objective appears to be **the dissemination of 'psychological' or disinformation warfare, in an attempt to generate chaos, panic and fear within the general population** so as to lower civilian morale, dissuade resistance and encourage surrender. For instance, several of the cyberattacks discussed above were accompanied by the posting of intimidating messages on computer systems such as 'Wait for the worst'.[17] Another example on March 16 was the hacking of Ukraine 24, a prominent media and TV channel, with the diffusion of false information claiming that Ukrainian President Volodymyr Zelensky had announced a surrender to Russia and was

[16] It should be noted that the same Russian-backed hacker group is suspected of being behind both of these cyberattacks, seven years apart.

[17] Przetacznik J. and Tarpova S., *Russia's war on Ukraine: Timeline of cyber-attacks*, European Parliamentary Research Service, June 2022.

asking the population to surrender as well; this was supplemented by a 'deep fake' video of Zelensky shared through a Telegram channel. As part of this psychological cyberwarfare, symbolism has also played a key role. For instance, in mid-March, hackers targeted several Ukrainian news outlets simultaneously, defacing their online platforms with a number of symbols banned in Ukraine, including communist-era symbols or Russian military war symbols (such as the St. George ribbon or the letters 'Z' and 'V'). Likewise, on April 22, a few days after the release of a new national stamp honoring a Ukrainian border guard, the country's national postal system was hit by a DDoS attack, which affected its online store. However, given the impressive scale of popular resistance from the Ukrainian people in opposing Russian forces since the beginning of the invasion, it appears that these types of psychological/ symbolic hackings and disinformation campaigns have not been successful in breaking civilian morale.

What is more, as the war has dragged on, **Russia's inability to conduct larger-scale cyberattacks** has been noteworthy. It appears that Russian hackers have re-focused their actions on mass espionage operations to collect sensitive data, probably in order to inform military operations on the ground. One of their preferred methods has been to rely on so-called 'phishing attacks' or 'trojan malware' to appropriate confidential information,[18] with multiple, successive waves of these cyberattacks launched not only against Ukrainian governmental and military entities, but also on financial institutions and various civilian targets. These types of spying operations, especially the phishing attacks, have been constant since the beginning of the invasion and amount to a form of cyber harassment. Prominent examples include phishing emails targeting military and governmental entities on March 17, the use of *LoadEdge* backdoor surveillance malware on March 20, as well as the *MarsStealer* information stealer on March 30 targeting the user credentials of citizens and various organizations. In April, these types of operations focused on governmental (April 2 and 7) and media entities (April 7), whilst also compromising private banking information (April 14) and payment data via a fraudulent social media survey (April 19). Such constant and sustained cyber espionage has continued over the following months and throughout the summer, possibly enabling Russian forces to obtain a certain amount of useful information in support of military operations. However, like other types of cyberattacks examined above, they appear to have yielded limited results on the whole, and have certainly not enabled any notable breakthrough for Russian forces in Ukraine. In fact, and for reasons that will be examined in more detail in the third section, most vital Ukrainian data, including sensitive military, governmental and financial information, has been kept safe throughout the war.

Finally, perhaps the most successful use of cyberattacks by Russia in the war so far has been the decision to engage in 'hybrid warfare', combining cyber operations in tandem with and in support of military strikes on the ground. Russia had already relied on this type of 'hybrid warfare' in the past during previous incursions into Georgia in 2008 and Crimea in 2014, albeit on a much smaller scale. 'Hybrid warfare' involves launching medium to low-scale precision cyberattacks against specific targets, such as a military, governmental, financial or media entity, in order to disable and incapacitate its computer systems, even if temporarily, in preparation for kinetic strikes from conventional military forces. The incapacitation of computer systems may generate chaos, fear and confusion, rendering the target

[18] 'Phishing' cyberattacks aim to trick users into downloading corrupt attachments or clicking on a link connecting them to a fraudulent website in order to infect computer systems with malware, often for spying purposes. Likewise, in reference to the Trojan Horse, a 'Trojan malware' lures users into downloading what appears to be a legitimate program but which in fact contains malicious code hidden within the software, in order to gain access to the user's computer system.

and surrounding ones more vulnerable and less able to defend against military strikes. Cyberattacks continue to play a vital role in this regard under a paradigm of 'hybrid warfare'. For instance, a number of the cyberattacks previously examined, especially those launched since March, have served to destabilize specific Ukrainian targets in preparation for kinetic military strikes from conventional Russian forces. One notable example was a cyberattack on the 7th of May targeting the Odesa City Council, with the aim to destabilize it just before and in parallel to the launching of missile strikes on the city's residential zones. Therefore, the current phase of the conflict in Ukraine has turned into what can be described as the world's first truly 'hybrid war'. Given that Russia's hybrid cyber-kinetic military offensive in the east of Ukraine yielded some results in the initial phase of the war, this carries important ramifications for the future of global warfare. It has highlighted the ways in which medium to low-scale precision cyberattacks against specific targets can be successfully combined with conventional military strikes and operations, with many countries around the world taking note of this.[19]

THE EXTERNAL CYBER DIMENSION OF THE WAR AND ITS IMPACT ON EUROPE: LIMITED SPILLOVER, LACK OF MAJOR CYBERATTACKS, AMPLIFICATION OF DISINFORMATION WARFARE AND INTERNATIONAL INVOLVEMENT

Due to the globalization of digital technologies, national boundaries and geographical distances are less relevant in the cyber realm. Consequently, a number of Russian cyberattacks targeting Ukraine over the past few years have spilled over to affect European countries, and even spread globally in some cases with devastating consequences, as with the *NotPetya* virus in 2017 (see first section). In addition, Moscow has already directly targeted Europe and the US with large-scale cyberattacks in the years leading up to the invasion, with several of the worst hackings believed to have originated from Russia (with the unprecedented *Solar Winds* cyberattack in 2020 being one of the latest such examples). For these reasons, there was widespread apprehension at the start of the latest phase of the Ukraine war that Europe and the US would once again be targeted by a wave of destructive cyberattacks.[20] The West's drastic economic sanctions against Russia could have invited cyber retaliation, with tensions running high and multiple threats being issued on both sides since the February invasion.

Like the internal cyber dimension of the war, however, the external cyber ramifications, while significant in a number of ways, have not unfolded as anticipated. The first surprise came from the rather limited spillover into Europe of the various cyberattacks which Russia unleashed against Ukraine. The most notable instance of spillover came on the very first day of the invasion with the hacking of the Viasat satellite company, which resulted in the disabling of modems connected to the Viasat Inc's KA-SAT satellite. While this contributed to disrupting communications within Ukraine (see above), there was also a spillover across Europe, impacting tens of thousands of people, businesses and governmental entities in a number of EU Member States from Poland to France. Even a month after the attack, disruptions were ongoing, with thousands of people still offline throughout Europe, including nearly 2000 wind turbines in Germany that remained disconnected and companies struggling to re-establish their connection with updated software.[21] This cyberattack triggered strong condemnation from US, EU and national officials, who released

[19] Lewis J. A., *Cyber War in Ukraine*, Center for Strategic and International Studies, June 2022.

[20] Kolbe P. R., Morrow M. R., and Zabierek L., *The Cybersecurity Risks of an Escalating Russia-Ukraine Conflict*, Harvard Business Review, 18 February 2022 (Updated on 24 February 2022).

[21] The cyberattack impacted people relying on satellite internet connection, as opposed to wired broadband cable connection (which still represents the majority of Internet connections). Likewise, it targeted the company's ground infrastructure, not the satellite in space.

statements confirming that intelligence pointed to a Russian-backed hacking.[22] Since then, however, there have not been any other comparable cyber spillovers into Europe from the war in Ukraine. One reason is the change in Russian cyber strategy, with Russia focusing instead on medium to low-scale cyberattacks as part of 'hybrid' military operations, including psychological warfare and persistent espionage (see above). This has considerably reduced the risk of cyber spillover into Europe. Other important factors responsible for this unexpected turn of events will be examined in more detail in the third section.

It is important to emphasize that, contrary to what many had anticipated, **Russia has for the time being conducted limited direct new cyberattacks against European countries and the US since the beginning of the invasion last February**. In fact, the ratio of cyberattacks affecting Western countries has only slightly increased over the last few months. Beyond Ukraine itself, Russia has focused many of its cyberattacks on Eastern European countries like Poland and Romania, which have served as major transit routes for the delivery of NATO weapons, equipment and various other humanitarian supplies to assist Ukraine. These countries have also provided important bases for the welcoming of Ukrainian refugees fleeing the war. For instance, on February 25, a destructive cyberattack targeted a border control station with the objective of hampering the flow of refugees into Romania, forcing local officials to manually process people crossing the border. Likewise, in late February, Russian-backed hackers targeted several European governments involved in the coordination of logistics for refugees, including Poland and Romania, with a phishing attack that relied on a comprised email address from a Ukrainian armed service member. In addition, the servers for a number of international NGOs, charities and aid organizations providing food, medicine and other basic relief to Ukrainians within the country and in neighboring EU member states, were hit by malware in early March that disrupted their online platforms. Between late April and early May, a number of government, bank, military and media websites in Romania were shut down following a series of DDoS attacks orchestrated by the pro-Russian hacker group 'Killnet'. These cyberattacks appear to have been in retaliation for a statement made by the President of the Romanian Senate at the time, Florin Cîțu, that his country was going to provide Ukraine with military equipment and act as a transit for NATO weapons. However, beyond these examples, there have not (yet) been large-scale direct cyberattacks against other EU member states or the US since the beginning of the Russian invasion – for reasons that will be examined in detail in the third section.

Instead, **Moscow has chosen to focus on amplifying its disinformation war against Europe and the West** more generally, relying on similar hacking methods as in the past (see above). While it is difficult to precisely identify this type of malevolent cyber activity, since it relies on indirect channels of communication like hacked or fake social media accounts, there is evidence of a notable increase in disinformation efforts targeting Western countries over the last few months.[23] Firstly, Russia has attempted to promote its own version of the narrative regarding the war in Ukraine, as constructed by the State propaganda apparatus. This involves claims about the war being merely a defensive response to NATO's expansion on Russia's border, and of the need to 'denazify' Ukraine by ridding it of its 'radical, far-right' govern-

[22] Corera G., *Russia hacked Ukrainian satellite communications, officials believe*, BBC news – 25 March 2022. See: https://www.bbc.com/news/technology-60796079

[23] Following the EU's ban of *Russia Today* and *Sputnik*, Russian hackers have endeavored to find new ways of spreading online disinformation in Europe and the West. See: Associated Press, *Russian Disinformation Spreading in New Ways Despite Bans*, Voice of America – 9 August 2022, https://www.voanews.com/a/russian-disinformation-spreading-in-new-ways-despite-bans-/6694083.html

ment. Unsurprisingly, this type of propaganda has not found a receptive audience in Ukraine, Europe or the US, where accurate reporting on the war has reached mass audiences.[24]

Yet, it is important to emphasize that Russia's disinformation war may have had more impact in other, and perhaps more devious ways. **Moscow appears to be seeking to capitalize on the fact that a notable proportion of citizens in Europe and the US could prove reluctant to continue supporting Ukraine when the economic costs of such support, including inflation and high energy prices, become more apparent over time.** Western countries are still recovering from the Covid crisis, hence the Ukraine war and its economic repercussions are adding further stress on an already fragile recovery. Over the last few months, Russia's disinformation has emphasized the high costs of supporting Ukraine, which may outweigh any potential and seemingly remote benefits. The aim has been to erode popular support for Kyiv, in an attempt to break Western unity and resolve from the inside. While the latter has not (yet) been successful, opinion surveys indicate that over the last few months, public opinion in Europe has begun to fracture. While solidarity towards Ukraine remains strong, a majority of citizens across most Member States now seem to be opposed to a protracted war due to concerns over the costs of economic sanctions and the threat of nuclear escalation, and only in a handful of countries is there substantial public support for boosting military spending.[25] It is difficult to attribute the degree to which this is due to the Russian disinformation campaign, or simply to a natural response in public opinion as the costs of the war have started to affect people more directly. Nevertheless, this is arguably a worrying trend, and one which certainly requires a more rigorous European and Western response (see next section for policy recommendations).

At the same time, due to Moscow's reliance on an amplification of its disinformation instead of large-scale direct cyberattacks against Europe and the West, there has been no need for substantive cyber retaliation against Russia. Consequently, NATO countries have yet to launch major new cyberattacks against Russian infrastructure, government, military or financial institutions since the war begun last February. Once more, however, this aspect of the cyber conflict resulting from the war in Ukraine has not unfolded in the way that many experts anticipated. Instead, and to the surprise of both sides, **Russia has been under constant cyber assault over the last few months from an international coalition of volunteer, non-governmental hacking organizations**, the most prominent being the 'Anonymous' movement.[26] The latter declared a cyber war against the Kremlin soon after the beginning of the invasion, conducting over the last few months one of the largest and most sustained cyber offensives ever launched against the Russian federation, and certainly the biggest operation in the movement's history. In addition to destructive cyberattacks, Anonymous has also sought to leak significant amounts of confidential information on Russian governmental, financial and military entities, and aimed to embarrass Putin's regime through a number of more symbolic hackings that have targeted the State propaganda apparatus. Some notable examples include the hacking of the Russian Central Bank and the space agency *Roscosmos*, the release of personal details on 120,000 Russian soldiers and military officers, breaking into the Kremlin's CCTV system, and hacking State media organizations (Russia-

[24] This has also been helped by the banning of Russian State media organizations like *Sputnik* or *Russia Today* across Europe shortly after the launching of the invasion.

[25] Krastev I. and Leonard M., *Peace versus Justice: The coming European split over the war in Ukraine*, *European Council on Foreign Relations*, Policy Brief – 15 June 2022.

[26] 'Anonymous' is a decentralized global hacktivist collective launched in 2003, which became famous for conducting a number of high-profile cyberattacks against governments or other types of institutions around the world, in support of various political causes.

24, Channel One or Moscow 24) by replacing scheduled content with videos of the Ukraine invasion. These high-profile attacks have run in tandem with more conventional cyberattacks on the country's critical infrastructure, including the shutting down of oil and gas pipelines. In another instance, Anonymous claims to have shut down over 1500 Russian and Belarusian websites from government, financial and State media institutions within a 72-hour period.[27] Moreover, several of the cyber operations launched by Anonymous were conducted in collaboration with Ukraine's so-called 'IT Army', a cyberwarfare organization created by Kyiv in late February 2022 made-up of volunteer hackers from both Ukraine itself and around the world (see details in the third section).[28]

It is difficult to determine the extent of the damage caused by these non-coordinated, often spontaneous cyberattacks which have targeted the Russian federation since the beginning of the invasion. While the disclosure of confidential information on Russian governmental, financial and military entities has been useful to Western intelligence agencies, at least to a certain extent, the quantity of data has been so massive that it could take months, perhaps even years to fully process. Nevertheless, Moscow might (inaccurately) interpret these spontaneous cyberattacks as having the covert backing of governments in Europe and the US, part of a disguised Western ploy to launch a direct cyber assault against Russia. Anonymous has certainly succeeded in embarrassing the Kremlin by shattering the myth about Russia's supposedly unbreakable cyber defenses. Hence, in order not to lose face, Russia could claim self-defense and retaliate against perceived Western aggression by launching largescale cyberattacks on EU member states and the US, with major risks involving a highly destructive escalation spiral. In fact, there is evidence of increased cyber espionage from Russian-backed hackers over the last few months targeting Western countries. Moscow appears to be probing the different possibilities and options for potentially launching more substantial cyberattacks in the near future, should the need arise and depending on the evolution of military operations on the ground in Ukraine, as discussed below.

III • Why the cyber dimension of the Ukraine war unfolded differently than expected and the policy consequences for Europe

ANALYSIS OF THE REASONS WHY THE CYBER DIMENSION OF THE WAR HAS UNFOLDED DIFFERENTLY THAN EXPECTED FOR UKRAINE AND EUROPE

There are many different reasons why the cyber dimension of the war has unfolded differently than expected, both within Ukraine, and in Europe or internationally. One of the main factors is that Russia simply underestimated Ukraine's cyber resilience, in the same way that it underestimated the country's armed forces, along with the determination of its government and civilian population to resist the invasion. Following the devastating series of cyberattacks which Russia unleashed against Ukraine during and after the events of 2014 (see first section), the Ukrainian government made it a top priority to reinforce national cyber defense capabilities and invested considerable resources in the process. This included upgrading Ukraine's Computer Emergency Response Team (CERT-UA), both in terms of budget and staff.

[27] In another highly symbolic move, Anonymous was also able to hack into the St. Petersburg International Economic Forum in June 2022, delaying President Putin's keynote speech by nearly 100 minutes.

[28] Interestingly, volunteer hackers from countries that are sympathetic to Moscow and generally hostile towards the US such as China, Belarus, Brazil, Iran and North Korea, have also been launching a series of spontaneous cyberattacks against Ukraine over the last few months to help Russian forces. Some of these hackings may have been supported, either directly or tacitly, by the governments of these countries.

Kyiv received substantial support from Western countries over the last few years, especially the EU and the US, including the transfer of IT equipment and software, along with extensive training and the provision of expertise.[29] In a number of cases, this has involved direct institutionalized cooperation between Western and Ukrainian governmental or military entities (see details below), universities, and the private sector. US-based companies like Microsoft, Amazon Web Services (AWS) and Google have played a key role in providing access to the latest upgraded cyber protection software.

European and US cyber assistance to Ukraine has accelerated since the beginning of the invasion last February, with US, UK and French security/military institutions, along with private firms like Microsoft, providing real-time cyber support to Ukraine. This has included warnings on imminent cyberattacks or direct intervention to neutralize Russian-backed hackings through online devices. Likewise, companies such as AWS and Microsoft have provided the Ukrainian government and armed forces with their own private Clouds, enabling the transfer of massive amounts of sensitive information to safe databases located outside the country (often within the US itself).[30] This has enhanced the country's remarkable cyber resilience since the beginning of the invasion, taking Moscow by surprise. Ukraine has stalled attempts by Russian hackers to launch several largescale cyberattacks, including the failed bid on April 8 to cut off the supply of electricity for millions of people by targeting power stations, where private sector entities once again provided key support on this occasion. Ukraine's cyber resilience has involved the creation of a specialized 'IT Army' two days after the start of the invasion, which has played a key role in thwarting Russia's attempted cyberattacks over the last few months. It is made-up of several thousand Ukrainian and foreign volunteer IT experts, who have launched a series of high-profile offensive cyberattacks against Russian forces and on Russia itself.[31] The IT Army has also concentrated efforts on bolstering cyber resilience and enhancing defenses within Ukraine itself, especially for critical infrastructure, governmental and military entities.

Another key factor impacting Ukraine's cyber resilience has been **the poor preparation of the Russian hackers** themselves. Indeed, CERT-UA and Western intelligence have confirmed that the vast majority of cyberattacks/hackings unleashed against Ukraine, as well as on Europe and the US since the beginning of the invasion, have simply involved updated versions of previous malware, with very few new viruses. This may be linked to Putin's gamble of a rapid or lighting military assault that would bring down Kyiv's democratically elected government in a matter of days. Hence, as with Moscow's lack of military preparations for protracted warfare on the ground, Russian-backed hackers appear to have been given insufficient advanced notice to develop new types of computer viruses. The latter can take months, even years to prepare, and must incorporate the planning of complex details for the cyberattack itself. Both Ukraine and the West were able to learn from their mistakes following previous large-scale Russian cyberattacks over the last few years. US intelligence, for example, has studied the types of cyber viruses relied upon by hackers with ties to Moscow and subsequently developed effective protections to bolster cyber resi-

[29] For instance, the US has invested as much as $40 million to help develop Ukraine's IT sector over the last few years.

[30] Cloud computing involves mobilizing internet servers often located in other countries (usually the US since many Cloud computing companies are based there) in order to store and process massive quantities of data, instead of relying on local servers or storage centers.

[31] This has included hacking the websites of the Moscow Stock Exchange and Sberbank (Russia's largest bank) on February 28, for example. Still, most offensive cyberattacks launched by Ukraine's IT Army have targeted Russian military forces, government websites in Russia and Belarus (including the FSB and State media agencies in both countries), along with power grids and railway networks to slow down or prevent Russian troops and equipment from reaching Ukraine.

lience. Thus, a good deal of the malware that Russia has mobilized against Ukraine and Europe since the beginning of the invasion has proven much less effective this time round.

Another compounding factor is linked to the impact of crippling Western economic sanctions imposed against Russia. The latter have rendered it much more difficult for hackers backed by the Kremlin to carry-out large-scale cyberattacks, especially those involving ransomware, since Russian entities have been cut off from the international financial and banking system. **The sanctions have also led to a hurried and drastic withdrawal of Western IT firms previously active in Russia, making it much more difficult for Moscow to access the latest IT equipment, software and expertise.** This is especially problematic in a rapidly evolving field like cybersecurity, where new developments are constantly taking place. A further, often underestimated factor has been the severe brain drain of Russian IT experts, especially young ones. An estimated 70,000 have already left their country since the invasion begun, fleeing the impact of the sanctions and in search of better opportunities abroad. At least 100,000 more are expected to leave over the next few months, which amounts to around 10% of Russia's total number of IT professionals and, more importantly, up to a third of its younger generation of experts.[32] Besides weakening Russia's cyber capabilities over the short run, this also raises serious questions about the country's ability to continue performing in this vital sector over the medium to long run.

Furthermore, in addition to factors outside the decision-making ambit of the Kremlin, the Russian government also appears to have deliberately adapted its cyber strategy, once the initial military invasion did not go according to plan. As explained above, it is now widely believed that Putin intended for a short 'special operation' that would rapidly bring down the regime in Kyiv in a matter of days. Since Ukrainian resistance and the unity of Western support took Moscow by surprise, Russian forces had not made sufficient preparations to secure their communication lines. Thus, they often had no other choice but to rely on local Ukrainian communications infrastructure from conquered territories. Consequently, any large-scale cyberattack, especially on Ukrainian communications, risked impacting Russia's reliance on local infrastructure for its war effort. What is more, the Kremlin had learned from *NotPetya* in 2017 that major cyberattacks can often slip out of control, since the virus had ended up spreading to Russia itself, affecting public institutions, banks, businesses, the media and various types of infrastructure across the country. Given the lack of preparation of the Russian military for a protracted war in Ukraine, combined with the crippling impact of Western economic sanctions, the Kremlin could not afford to risk a similar type of large-scale cyberattack which might cause as much harm to Russian forces as Ukrainian ones. As a result, Moscow adapted its cyber strategy to focus on medium to low-scale targeted cyberattacks as part of hybrid military operations on the ground, comprised of extensive cyber espionage, psychological warfare in Ukraine along with an amplification of its disinformation campaign against the West. This was clearly a more realistic approach than engaging in all out-all cyber war, with the concomitant risks of spillover and retaliation.

In this regard, **fear of Western retaliation appears to have been an important factor in dissuading the Kremlin from launching any major cyberattack against Europe and the US since the outbreak of the war**. NATO has warned Putin multiple times that any significant cyberattack against a member state would trigger a substantive, collective response. The Alliance has significantly bolstered its cyber

[32] These statistics come from the Russian government itself, which means that the real number might be even higher. See: The Moscow Times, *170 thousand Russian IT Specialists Could Emigrate by April – Industry*, 19 April 2022.

capacities over the last few years (both offensive and defensive), with the cyber sphere now constituting a top priority where Allies have decided to invest sizeable resources, as for land, sea and air combat.[33] What is more, NATO has been somewhat vague, perhaps deliberately, about the potential links between a large-scale cyber-attack on a member country and the triggering of Article 5 of the Alliance Treaty, whereby an attack on one is considered as an attack on all. NATO's Secretary General Stoltenberg has indicated that certain types of major cyberattacks might be considered as an act of war and could thus lead in some circumstances to a triggering of Article 5.[34] Unsurprisingly, President Putin has also made similar threats over the last few months about the consequences of NATO launching a direct large-scale cyberattack against Russia to support Ukraine. Since the latter could potentially result in direct military confrontation between NATO and Russia, with unpredictable consequences between the world's foremost nuclear powers, a new military doctrine based around 'mutually-assured destruction' in the cyber realm, or 'cyber-MAD', has arguably emerged from the latest phase of the Ukraine war, ushering in what can be described as a 'cyber Cold War'. This represents a highly significant development in relations between Russia and the West, with the new cyber-MAD complementing the previous nuclear-MAD doctrine inherited from the (first) Cold War.[35]

THE RISKS OF ESCALATION AND POLICY RECOMMENDATIONS FOR THE EU IN RESPONSE TO THE CYBERSECURITY RAMIFICATIONS OF THE UKRAINE WAR

The EU has provided Ukraine with various types of assistance to help it bolster its cyber defenses, including the transfer of equipment, software and the provision of expertise. This has taken place through frameworks such as the 'EU-Ukraine cyber-dialogue', launched in June 2021 and subsequently enhanced following the Russian invasion. This dialogue has reinforced the operational capacity of Ukraine's telecommunications sector and played a role in tackling Moscow's disinformation campaign. Likewise, in response to a request from the Ukrainian government, the EU decided for the first time in February 2022 to activate its 'Cyber Rapid Response Teams' (CRRTs) under an operational context, which function via the 'permanent structured cooperation' (PESCO) framework. The EU's CRRTs are composed of cyber expert volunteers from six member states (Netherlands, Poland, Lithuania, Romania, Estonia and Croatia) to be deployed across Europe. The aim is to help Ukraine defend itself from cyberattacks through the provision of assistance, as well as cyber recognition, threat detection and mitigation. The EU also imposed the first-ever set of sanctions in July 2020 targeting a number of Russian hackers thought to be behind the series of cyberattacks that have impacted Ukraine and Europe over the last few years (like the *NotPetya* virus). Moreover, the US Cyber Command has started to cooperate with the EU's CRRT in searching for active cyber threats, whilst NATO allies have reinforced cyber information-sharing with Kyiv, along with actual support on the ground. Ukraine has become a contributing participant of NATO's 'Cooperative Cyber Defence Centre of Excellence', in addition to enhanced cooperation with the 'European Centre of Excellence for Countering Hybrid Threats'

[33] In this regard, NATO has been organizing since 2010 an annual large-scale cyber exercise referred to as *Locked Shields*, which simulates a coordinated response to a major cyberattack on a member country.

[34] *Russia-Ukraine conflict: NATO chief warns Russia that cyber attacks can trigger NATO Charter Article* 5, Global News, 25 February 2022. See: https://globalnews.ca/video/8646550/russia-ukraine-conflict-nato-chief-wars-russia-that-cyber-attacks-can-trigger-nato-charter-article-5

[35] The concept of 'cyber-MAD' refers to two separate, yet interrelated elements. First, it points to the risk of cyber escalation that could lead to the outbreak of a large-scale cyber world war involving major cyberattacks launched by both NATO and Russia, with devastating consequences. The second element, which is directly related to the first, is that the outbreak of such a cyber world war may lead through a chain of events to a kinetic world war and direct military confrontation between NATO and Russia over Ukraine.

following the outbreak of the war, with the organization of joint exercises for example.

These measures are significant and have certainly played a key role in terms of bolstering Ukraine's cyber defenses. As examined in the previous section, Russia has failed in its attempts to launch large-scale cyberattacks against Ukraine since the beginning of the invasion, in large part due to Kyiv's remarkable cyber resilience. Nevertheless, this is no reason for complacency. The war in Ukraine has not gone as the Kremlin planned, and the current Ukrainian counter-offensive appears to have put Russian forces on the defensive. If Moscow were to continue losing control over previously conquered territories during the coming months, the Kremlin might become desperate enough to launch renewed attempts at large-scale cyberattacks against Ukraine, despite the risk of spillover to its own forces and Russia itself. Therefore, it is essential for Europe to enhance its support for Ukraine in terms of cybersecurity. Firstly, this should take the form of greater coordination between the EU's CRRT and US Cyber Command which, despite initial cooperation in searching for active cyber threats, have yet to develop more structured collaboration in their provision of assistance to Ukraine. Secondly, it would be beneficial for the EU to consider including associated 'Eastern Partnership' (EaP) countries like Ukraine, Moldova and Georgia that have association agreements with the EU, in the framework of individual 'permanent structured cooperation' projects focusing on cybersecurity and hybrid risks. This could lead to the development of civilian cyber operations, and might involve expanding the mandate of the EU's Advisory Mission in Ukraine to address threats relating to cybersecurity, including in the areas of digital technologies and strategic communications.[36]

Moreover, it is important to emphasize that the risk of cyber escalation is not limited to the internal situation in Ukraine. Indeed, if Russia were to make renewed attempts at launching major cyberattacks against Ukraine in the near future, there is a real risk of spillover into Europe and the West more generally, as exemplified by the *NotPetya* virus in 2017 (see first section). In this regard, the government in Kyiv has highlighted that more than 100 of the world's Fortune 500 companies depend at least in part on Ukrainian IT services (software engineers, code writers or hosted services), with a non-negligeable number of Ukrainian IT firms belonging to the top 100 global outsourcing options for IT services. In addition to the risk of spillover, there is also the possibility of Russia suddenly deciding to launch major cyberattacks directly against Europe and Western countries, as it has in the past (with the *Solar Winds* hacking in 2020 being the latest such example – see first section). As previously explained, a number of different factors have converged to explain why this has not yet happened since the beginning of the invasion last February. However, many experts have warned that President Putin considers the war in Ukraine to be one which he cannot afford to lose. Thus, should the military situation on the ground evolve in favor of Kyiv and Moscow feels that its back is against the wall, it would be easy to blame this on the West in order to justify a more serious escalation.[37] While some fear reliance on nuclear weapons, the risk of the latter happening remains low due to the prospect of mutually assured destruction. **A less perilous strategy for Putin might be to try and launch a full-scale cyber assault against Europe and the West as a desperate last resort, in spite of the devastating consequences this would entail for Russia due to cyber retaliation**, and the possibility of this

[36] The European Parliament issued a resolution on the 8th of June concerning security in the Eastern Partnership area in relation to the Common Security and Defence Policy, which highlighted several of these policy recommendations.

[37] In this regard, Putin and Russian officials have already been escalating their rhetoric by blaming Russia's sluggish military progress in Ukraine on NATO interference in the conflict and on the West supplying weapons to Kyiv.

leading to direct military confrontation. The risk of misunderstanding or strategic miscalculation triggering a dangerous escalation is genuine, especially due to the involvement on both sides of international hacking organizations like Anonymous, which governments have trouble controlling (see previous section).

Therefore, **it is essential that Europe not let down its guard down by continuing to reinforce cyber resilience in the near future, including with additional efforts to tackle ongoing Russian disinformation campaigns**. Over the course of the last few years, the EU has enacted a number of policies and legislation in the area of cybersecurity. For example, the 2016 Directive on the Security of Network and Information Systems (NIS) represents the primary legislative framework for the cybersecurity of critical infrastructure. It led to the development of common EU-level standards for 'operators of essential services' (OES), covering a wide range of vital infrastructure. This was followed by an EU Cybersecurity Act in 2019, which reinforced procedures for implementing the NIS Directive, and introduced an EU-wide certification framework for a broad range of digital goods and services. While these certainly constitute notable improvements, the fact remains that the EU has not invested enough in tackling online disinformation (which is only peripherally addressed in the above-mentioned laws). Because the EU's approach to cybersecurity is characterized by 'flexibility', Member States have often been given wide latitude for enacting EU standards.[38] Under the NIS directive, each Member State must develop its own national cybersecurity strategy. While an EU cybersecurity strategy was presented in 2013 and updated in 2020, it remains limited to the provision of general policy suggestions, which means that governments are left with the responsibility of developing their own detailed rules at the national level. Member States are required under the NIS Directive to develop a 'Computer Security and Response Team' (CSIRT), assembled under a common European network, together with a 'Cooperation Group' including the EU Commission and national cyber agencies. However, much like the EU Agency for Cybersecurity[39], none of these various frameworks or institutions possess sufficient competences, like sanctions, to enforce compliance with EU-level cyber norms. Reinforcement capacity is attributed instead to Member State authorities, which may choose to provide the degree of authority they deem appropriate to national CSIRTs. The end result has been the emergence of significant disparities in the effectiveness of national cybersecurity frameworks, with a highly differentiated paradigm for countries across the EU. Such a multi-speed Europe is particularly problematic in the realm of cybersecurity, due to the high degree of interconnection between Member States resulting from their membership in the Single Market, which encompasses digital technologies. Hence, countries with less developed cybersecurity frameworks constitute 'weak links' which may allow for malware to penetrate their national computer network, before propagating to other Member States and potentially compromising the whole EU system.[40] Such a scenario has in fact already taken place on several occasions during previous Russian-backed cyberattacks targeting Ukraine and/or Europe (see first section).

As a result, implementation of the NIS Directive has been challenging, leading to notable fragmentation across the Single Market at different echelons. The EU Commission responded with a proposal to upgrade the NIS Directive, with final agreement on the new legislation reached in May 2022. The second NIS Direc-

[38] Barichella (2018).

[39] Formerly known as ENISA, the EU Agency for Cybersecurity received a permanent mandate, an increased budget along with new policy tools after passage of the 2019 Cybersecurity Act. Yet, the Agency's competences remain limited to advising Member States and fostering collaboration, along with analyzing and sharing data.

[40] Barichella (2022).

tive seeks to bolster cybersecurity requirements, address the security of supply chains, reinforce obligations for reporting, along with a general strengthening of enforcement procedures with better supervision, including through an improved harmonization of sanctions across countries. NIS 2 also aims to significantly expand the number of sectors and entities encompassed by the legislation compared to the original directive, with the objective of an alignment with sectors covered by EU standards for the protection of physical infrastructure.[41] The NIS 2 Directive clearly represents a much-needed upgrade of the EU's cybersecurity framework, especially in light of the ongoing war in Ukraine. Once again, however, the new legislation only indirectly tackles online disinformation, and may also not go far enough in terms of addressing the problem of weak links. For instance, despite the initiative on more harmonization of sanctions, Member States are still left with the responsibility to develop detailed rules for their own national cybersecurity paradigms; this may sustain problems linked to the differentiation of norms throughout the EU.[42] In this regard, the announcement of a new 'Strategic Compass' in June 2022, which aims to strengthen the EU's collective security and defense by 2030, offers several interesting policy perspectives. The Strategic Compass proposes to enhance Europe's cybersecurity through the elaboration of a new 'cyber resilience act', an expansion of the EU's 'Cyber Diplomacy Toolbox', along with closer collaboration with the Union's eastern partners in addressing hybrid threats, including disinformation. These suggestions hold potential, and it is essential to translate them into concrete policies and legislation over the next few years. Priorities should include the tackling of disinformation, addressing the issue weak links across Member States and reinforcing cybersecurity collaboration with Ukraine, core proposals for an upgraded and enhanced EU cyber strategy.

Bibliography

Accenture, *Global Incident Report: Russia-Ukraine Crisis*, 10 June 2022.

Associated Press, *Russian Disinformation Spreading in New Ways Despite Bans*, Voice of America, 9 August 2022.

Barichella A., *European Cybersecurity and Data Privacy: Threats and Prospects*, Policy Brief – Jacques Delors Institute, March 2022.

Barichella A., *Cybersecurity in the Energy Sector: A Comparative Analysis between Europe and the United States*, Études de l'Ifri, February 2018.

Corera G., *Russia hacked Ukrainian satellite communications, officials believe*, BBC news, 25 March 2022.

Costigan S. and Tagarev T., *Countering Crime and Disinformation in Cyberspace,* Connections: The Quarterly Journal, Vol. 20 No. 2, Spring 2021.

Cyber Peace Institute, *Ukraine: Timeline of Cyberattacks on critical infrastructure and civilian objects, last updated on 8 June 2022.*

Dubov D., *The War in Cyberspace: Russia's War in Ukraine* (Series No. 2), International Centre for Defence and Security, May 2022.

Kagubare I., *What the Russia-Ukraine war means for the future of cyber warfare*, The Hill, 20 June 2022.

Kolbe P. R., Morrow M. R., and Zabierek L., *The Cybersecurity Risks of an Escalating Russia-Ukraine Conflict, Harvard Business Review, 18 February 2022 (Updated on 24 February 2022).*

[41] In June 2022, an agreement was reached for a new Directive on the resilience of critical entities, which involves strengthening EU standards for physical infrastructure; these differ from cybersecurity norms, covered by the NIS Directive. The objective is to align sectors between these two directives, covering transport, health, drinking water, waste water, energy, banking and financial markets, along with digital infrastructure and outer space.

[42] Barichella (2022).

Krastev I. and Leonard M., *Peace versus Justice: The coming European split over the war in Ukraine*, European Council on Foreign Relations, Policy Brief – 15 June 2022.

Fendorf K. and Miller J., *Tracking Cyber Operations and Actors in the Russia-Ukraine War*, Council on Foreign Relations, 24 March 2022.

Global News, *Russia-Ukraine conflict: NATO chief warns Russia that cyber attacks can trigger NATO Charter Article 5*, 25 February 2022. See: https://globalnews.ca/video/8646550/russia-ukraine-conflict-nato-chief-wars-russia-that-cyber-attacks-can-trigger-nato-charter-article-5

Gould J., *No. 2 Senate Democrat decries alleged Russian hack as 'virtual invasion'*, C4ISRNet, 17 December 2020.

Lewis J. A., *Cyber War in Ukraine, Center for Strategic and International Studies*, June 2022.

Madnick S., *What Russia's Ongoing Cyberattacks in Ukraine Suggest About the Future of Cyber Warfare*, Harvard Business Review, 7 March 2022.

Quallo-Wright M., *Preparing for the long haul: the cyber threat from Russia*, UK National Cyber Security Centre, 5 July 2022.

McLaughlin J., *A digital conflict between Russia and Ukraine rages on behind the scenes of war*, National Public Radio, 3 June 2022.

Orenstein M., *Russia's Use of Cyberattacks: Lessons from the Second Ukraine War*, Foreign Policy Research Institute, 7 June 2022.

Peacock R., *How Ukraine has defended itself against cyberattacks – lessons for the US*, The Conversation, 5 April 2022.

Pearson J. and Bing C., *The cyber war between Ukraine and Russia: An overview*, Reuters, 10 May 2022.

Pipikaite A. and Bester L., *How the cyber world can support Ukraine, World Economic Forum*, 19 March 2022.

Przetacznik J. and Tarpova S., *Russia's war on Ukraine: Timeline of cyber-attacks*, European Parliamentary Research Service, June 2022.

Rosen K. R., *The Man at the Center of the New Cyber World War*, POLITICO, 14 July 2022.

Shchyhol Y., *Vladimir Putin's Ukraine invasion is the world's first full-scale cyberwar*, Atlantic Council, 15 June 2022.

The Moscow Times, *170 thousand Russian IT Specialists Could Emigrate by April – Industry*, 19 April 2022.

UNHCR, *Operational Data Portal: Ukraine Refugee Situation*. See: https://data.unhcr.org/en/situations/ukraine

Managing Editor: Sébastien Maillard • The document may be reproduced in part or in full on the dual condition that its meaning is not distorted and that the source is mentioned • The views expressed are those of the author(s) and do not necessarily reflect those of the publisher • The Jacques Delors Institute cannot be held responsible for the use which any third party may make of the document • Original version • Edited by Anne-Julia Manaranche • © Jacques Delors Institute

Institut Jacques Delors
Penser l'Europe • Thinking Europe • Europa Denken
18 rue de Londres 75009 Paris, France • www.delorsinstitute.eu
T +33 (0)1 44 58 97 97 • info@delorsinstitute.eu

NOTRE EUROPE
Jacques Delors Institute
Penser l'Europe • Thinking Europe • Europa denken

PREMIER MINISTRE
Liberté
Égalité
Fraternité

L'Europe pour les citoyens