ISSN 2421-4442

SICUREZZA TERRORISMO SOCIETÀ

Security Terrorism Society

INTERNATIONAL JOURNAL - Italian Team for Security, Terroristic Issues & Managing Emergencies

15
2022

EDUCatt

SICUREZZA, TERRORISMO E SOCIETÀ

INTERNATIONAL JOURNAL
Italian Team for Security,
Terroristic Issues & Managing Emergencies

15

ISSUE 1/2022

Milano 2022

EDUCATT - UNIVERSITÀ CATTOLICA DEL SACRO CUORE

SICUREZZA, TERRORISMO E SOCIETÀ
INTERNATIONAL JOURNAL – Italian Team for Security, Terroristic Issues & Managing Emergencies

ISSUE 1 – 15/2022

Direttore Responsabile:

Matteo Vergani (Università Cattolica del Sacro Cuore – Milano e Global Terrorism Research Centre – Melbourne)

Co-Direttore e Direttore Scientifico:

Marco Lombardi (Università Cattolica del Sacro Cuore – Milano)

Comitato Scientifico:

Maria Alvanou (Lecturer at National Security School – Atene)
Cristian Barna ("Mihai Viteazul" National Intelligence Academy– Bucharest, Romania)
Claudio Bertolotti (senior strategic Analyst at CeMiSS, Military Centre for Strategic Studies – Roma)
Valerio de Divitiis (Expert on Security, Dedicated to Human Security – DEDIHS)
Chiara Fonio (Università Cattolica del Sacro Cuore – Milano)
Sajjan Gohel (London School of Economics – London)
Rovshan Ibrahimov (Azerbaijan Diplomatic Academy University – Baku, Azerbaijan)
Daniel Köhler (German Institute on Radicalization and De-radicalization Studies – Berlin)
Miroslav Mareš (Masaryk University – Brno, Czech Republic)
Vittorio Emanuele Parsi (Università Cattolica del Sacro Cuore – Milano)
Anita Perešin (University of Zagreb – Croatia)
Giovanni Pisapia (Senior Security Manager, BEGOC – Baku – Azerbaijan)
Iztok Prezelj (University of Ljubljana)
Eman Ragab (Al-Ahram Center for Political and Strategic Studies (ACPSS) – Cairo)
Riccardo Redaelli (Università Cattolica del Sacro Cuore – Milano)
Mark Sedgwick (University of Aarhus – Denmark)
Arturo Varvelli (Istituto per gli Studi di Politica Internazionale – ISPI – Milano)
Kamil Yilmaz (Independent Researcher – Turkish National Police)
Munir Zamir (Fida Management&C7 – London)
Sabina Zgaga (University of Maribor – Slovenia)
Ivo Veenkamp (Hedayah – Abu Dhabi)

Comitato Editoriale:

Gabriele Barni (Università Cattolica del Sacro Cuore – Milano)
Alessia Ceresa (Università Cattolica del Sacro Cuore – Milano)
Barbara Lucini (Università Cattolica del Sacro Cuore – Milano)
Marco Maiolino (Università Cattolica del Sacro Cuore – Milano)
Davide Scotti (Università Cattolica del Sacro Cuore – Milano)

© 2022 EDUCatt - Ente per il Diritto allo Studio Universitario dell'Università Cattolica
Largo Gemelli 1, 20123 Milano - tel. 02.7234.22.35 - fax 02.80.53.215
e-mail: editoriale.dsu@educatt.it (produzione); librario.dsu@educatt.it (distribuzione)
web: www.educatt.it/libri

Associato all'AIE – Associazione Italiana Editori

ISSN: 2421-4442
ISSN DIGITALE: 2533-0659
ISBN: 978-88-9335-956-6

copertina: progetto grafico Studio Editoriale EDUCatt

Sommario

The importance of the Cyber battleground in the Russo-Ukrainian war

Marco Zaliani

Marco Zaliani is analyst and researcher at the Italian Team for Security Terroristic Issues and Managing Emergencies – ITSTIME. He has a BA in Foreign Languages for Business at Università Cattolica del Sacro Cuore (UCSC) and Master in International Relations at ASERI – Postgraduate School of Economics and International Relations (UCSC), with a final thesis titled: "Information warfare: The new frontier of international hybrid conflicts". He specialized in Cyber Security analysis, Open Source Intelligence (OSINT) and social network analysis. He focused on monitoring terrorist propaganda and relevant threats regarding national security, with particular attention on Cyber Warfare and threats posed by terrorist and extremist organizations. His research work includes: analysis of threat trends and scenarios regarding in particular on Islamic terrorism, right-wing extremism, Cyber Warfare and national security issues in general.

Abstract

The increasingly hybrid nature of conflicts has become even more evident in the recent re-ignition of the never-dead Russian-Ukraine crisis. The new chapter of this conflict, which arose from the Russian military invasion of Ukrainian territory, was characterized by massive use of hybrid instruments of the conflict that went hand in hand with the military one. In this context, the cyber dimension of the conflict has reaffirmed its central role. As it is now an integral part of these conflicts and no longer ancillary to them. Starting from a study of the implementation of cyber-arsenals used in the Ukrainian context, we want to give a more precise image of this type of weapons which, just like conventional arsenals, are exploited to achieve specific objectives by a variety of actors. In fact, in this conflict, the "cyber-line ups" that have seen state and non-state actors intervening alongside both Russia and Ukraine are also indicative.
From these considerations, one can get an idea of the current role of cyber in the context of new hybrid conflicts and specifically outline the scenarios that the Russo-Ukrainian conflict may cause in cyberspace even after hostilities are over.

Keywords

Ukraine, cyber, hybrid warfare

1. Introduction of Cyber warfare in Ukraine

The recent invasion of Ukraine conducted by Russian military forces at the end of February 2022 has sparked new fears of a conflict at Europe's door and cold war-like sentiment. Apart from the obvious military aspect of the invasion, there is one aspect that has gained increasing importance over the years which is Cyber Warfare. Since the beginning of the ongoing Russian military operation in Ukraine, it has played a central role in the conflict, and it was exploited by both sides in many ways. This is not the first time, however, that Ukraine has been at the epicenter of Russian Cyber efforts. Very much like the Baltic states, Ukraine has been over the years a sort of "testing ground" in which Russians could deploy their newest Cyber weapons. This was done both to send a message to the West regarding Russian capabilities and what to expect if a conflict breaks out in Cyber space, and at the same time to project themselves even more towards Ukraine which has a key role in the stability of the region. In 2015 and 2016 Ukrainian power-grids were subject to multiple attacks. The 2015 attack was conducted by the Russian APT (Advanced Persistent Threat) "Sandworm" using the Trojan "BlackEnergy" on energy companies in Ukraine and resulted in power outages that lasted up to six hours. Ukraine was also a major target of the malware epidemic caused by NotPetya, a destructive ransomware that targets Microsoft operating systems and encrypts everything on the hard drive. If infected by NotPetya it is technically impossible to recover the encrypted files even after the payment in BitCoin. The attack was again attributed to the Russian APT Sandworm. These major hacks were all interspersed by various less severe ones like DDoS and defacements targeting the Ukrainian government's websites. Therefore, over the years it has become evident that Cyber Warfare has been used plenty of times in Ukraine as an integral part of the war and this new phase of the conflict with Russia could not be outdone.

2. Cyber Weapons used

Much like a real battlefield, cyberspace has seen different types of weapons being used too. Their characteristics range from pure disinformation and influence to actual compromise and intrusion followed by data leaks. The following is meant to give an outline of this range of severity of the attacks that have been witnessed so far in the conflict.

- Starting from the least severe type of attacks, various **Phishing** campaigns have been recorded. Even though it must be said that Phishing can be, and oftentimes is, just a vector of more serious attacks, in Ukraine various

Phishing campaigns have been launched to force narratives on the population and influence it.

For example, at the end of February, Meta said it has seen a surge in hacking attempts against Ukrainians. It identified some from a threat actor that has been trying to hack the accounts of high-profile Ukrainians, including military officials and public figures. The threat actor typically targets people through phishing emails and then uses that to gain access to their social media accounts and post disinformation as if it is coming from the legitimate account owners. Hence, even if the attacks did not lead to major disruptions, they still tried to influence the Ukrainian population in any way possible, just like the Russian InfoWar tactics predict.

- Moving up the severity scale a different and a lot less subtle way of influence was used from both the Russian and the Ukrainian sides. That is **Defacement** of institutional and commercial websites. Website defacement is a form of "electronic vandalism" with which the visual appearance of a website or a web page is changed and/or modified with satirical or misleading content. The Hacktivist group Anonymous has long been a user of such technique and it has used it also in this conflict against Russia. They have hacked into the networks of Russian state television, and they showed the reality of the atrocities that were being committed in Ukraine. This again is an example of how cyberwarfare can be used to influence the public debate also from a defensive side like Anonymous did in defense of Ukraine.[1]
- The next cyber weapon used is one of relative ease of use and it has been exploited massively by both sides of the conflict. The weapon in question is a **DDoS** attack or "Distributed Denial of Service". This kind of attack is conducted through the flooding of a target IP (a website) with thousands of requests. If there are not enough defenses against this kind of attack the requests become too many for the webserver to handle and the website becomes unreachable. This technique has been used extensively both by Russia, targeting institutions, Banks, and other commercial entities[2] and by Ukraine also through its IT cyber army and its cyberspace allies like Anonymous.[3] In the case of Russian DDoSs, even though the scale of the attacks was moderate, and the sites recovered within hours, the clear intention was to create a sense of panic in the population that was not able to gather neither information or money.

[1] https://fortune.com/2022/03/07/anonymous-claims-hack-of-russian-tvs-showing-putins-ukraine-invasion/

[2] https://www.reuters.com/world/us-says-russia-was-responsible-cyberattack-against-ukrainian-banks-2022-02-18/

[3] https://www.theguardian.com/world/2022/feb/27/anonymous-the-hacker-collective-that-has-declared-cyberwar-on-russia

- The next tool in the cyber arsenals is more pervasive and bears highly destructive characteristics. During the last months, a very large use of **Wiper**-type Malwares has been detected. Wiper Malwares are a specific kind of Malware that, once it is delivered into the victim's machine, erases user data and partition information from attached drives. At least three different Wiper Malwares have been identified in Ukrainian networks. The researchers named them Isaac Wiper, Hermetic Wiper, and Caddy Wiper.[4] Most of them required a previously established presence in the target's network, but once inside they proceeded to do the "wipe" of all the data that resulted in major problems for the entities involved. Hermetic Wiper for example has been described by researchers as remarkable for its ability to bypass Windows security features and gain write access to many low-level data-structures on the disk. In addition, the malware was set to fragment files on disk and overwrite them to make any attempt of recovery impossible.[5]
- One special mention regards the use of **Ransomware**. This kind of attack is similar to the previous one on the list, but it is normally used for financial gains since it involves a "ransom". Nevertheless, it was used by hacker groups this time to put political pressure on the enemy, making it the first use of ransomware as a hybrid warfare tool.[6]

3. Cyber line ups

The involvement of Ransomware groups in the Russo-Ukrainian conflict is another hint of the growing hybridization of conflicts. After the beginning of hostilities, several actors have picked sides and started fighting, this time however in cyberspace and not with bullets. The following are the main groups and entities, both state and non-state, that have taken part in the conflict.

Pro Ukraine groups:

- **Anonymous**: The group of hacktivists has been one of the most outspoken defiant of the Russian government. On the 24th of February they officially declared war against Russia via one of their Twitter accounts. Since then, the collective has started hitting Russian state TV networks and other governmental websites like the one of the Ministry of Defense.[7] The latter has

[4] https://securityintelligence.com/posts/caddywiper-malware-targeting-ukrainian-organizations/
[5] https://blog.malwarebytes.com/threat-intelligence/2022/03/hermeticwiper-a-detailed-analysis-of-the-destructive-malware-that-targeted-ukraine/
[6] https://www.atlanticcouncil.org/blogs/belarusalert/cyber-partisans-target-russian-army-in-belarus-amid-ukraine-war-fears/
[7] https://www.theguardian.com/world/2022/feb/27/anonymous-the-hacker-collective-that-has-declared-cyberwar-on-russia

not only been put offline, but its database was also compromised and then leaked online by Anonymous. Out of 100 misconfigured databases in Russia, 90 were compromised and leaked by Anonymous.[8] The group's leaderless nature makes attribution even harder. Russia tried to link the group to some sort of American support, given the fact that most of the 17.000 IP detected and shared by the Russians were US-based.[9] The group's dispersed nature and the relative user-friendly attacks it employs make it a tough adversary for Russia as it has been for the US when it was targeting American companies.

- **IT Cyber Army of Ukraine**: This is a prime example of the hybrid nature of the current conflict. The newly formed group has been launched by the vice-prime minister of Ukraine Mykhailo Fedorov, to fight against Russian digital intrusions and it was open to any cyber-expert would want to join. It is probably the first case in which a government openly calls for the creation of a cyber-volunteer unit from all over the world to participate in a conflict.[10] In the announcement made by Fedorov, a link for a Telegram channel was also provided to coordinate attacks and to give a list of Russian entities' IP addresses to target. In the channel a series of guides and manuals were also shared, so that anyone could participate and launch DDoS attacks.
- **Belarusian Cyber Partisans**: The Belarus-based group isn't new to politically motivated attacks. It has a long story of hacks that targeted primarily Lukashenko's regime. Given Belarus' historic alliance and vicinity to Russia the group decided, both before and after the beginning of the invasion, to deploy its ransomware against targets inside Belarus.[11] Before the invasion the group hacked into the Belarusian Railways computer system in a bid to sabotage the deployment of Russian military units in the country and again hit the same target after the military operations started. The episode was interesting because it was one of the first cases in which ransomwares were used to pursue a political objective and not a financial one.

Pro Russia Groups:

- **Sandworm (Unit 74455)**: This APT is among those actors that have intervened alongside Russia. While the Russians have always denied any link

[8] https://www.cnbc.com/2022/03/16/what-has-anonymous-done-to-russia-here-are-the-results-.html

[9] https://www.bleepingcomputer.com/news/security/russia-shares-list-of-17-000-ips-allegedly-ddosing-russian-orgs/

[10] https://www.reuters.com/world/europe/ukraine-launches-it-army-takes-aim-russian-cyberspace-2022-02-26/

[11] https://www.atlanticcouncil.org/blogs/belarusalert/cyber-partisans-target-russian-army-in-belarus-amid-ukraine-war-fears/

with the group it is strongly believed that it is in fact a cyber-offensive unit of the Russian GRU, the government agency in charge of Russian Military Intelligence.[12] The group is known for the high sophistication of its hacks and has been involved in many large-scale hacks like the previously cited NotPetya. Sandworm has been reportedly targeting Ukrainian networks with a new malware dubbed by researchers "Cyclops Blink".[13]

- **Ghostwriter (UNC1151):** This threat actor is another state-sponsored group. It has been linked with high confidence to the Belarusian government and has too been active in the Russo-Ukrainian conflict. Meta has reportedly taken down several accounts on its platforms that are linked to the group.[14] These accounts were being used to target those of Ukrainian officials and military personnel. This was done to compromise them and disseminate false information regarding the conflict as if it was coming from the legitimate Ukrainian profiles.
- **Conti:** The ransomware group has, like Anonymous, officially declared that it was going to take part in the conflict alongside Russia and defend it from any outside attack. Like in the case of the Belarusian Cyber Army a ransomware group has put aside financial gains to pursue politically driven objectives. The support to Russia though backfired when a pro-Ukraine member of the group has started to leak various internal data through a twitter profile whose handle is @ContiLeaks. The leaks included the logs for the internal group chat, the entirety of Conti ransomware group's victims' data and even the source code of its ransomware and its decryptor. The group is one of the most successful "ransomware gangs", and, since in the leaks were also the bitcoin wallets used to collect ransoms, it has been calculated that between 2017 and 2022 it has netted around two and a half billion dollars in BitCoin from ransom payments.

4. Consequences of Cyber Warfare in Ukraine and future scenarios

The hybridization of conflicts has become more and more evident in the recent clash between Russia and Ukraine. The weapons used, the actors involved and the dynamics that were created thanks to one or the other projected the west in a new phase of modern confrontations between states. A

[12] https://www.theverge.com/21344961/andy-greenberg-interview-book-sandworm-cyber-war-wired-vergecast

[13] https://www.siliconrepublic.com/enterprise/ukraine-cyberattacks-ddos-hermetic-cyclops-russia-invasion

[14] https://www.bleepingcomputer.com/news/security/meta-ukrainian-officials-military-targeted-by-ghostwriter-hackers/

phase in which, even when military clashes are over, the conflict inevitably continues in cyber-space in the form of espionage, influence, and sabotage. This (most of the times) low-intensity war in cyber-space can bring devastating consequences if states are not ready to face it. Even if, also in Ukraine, cyber-attacks have not been as devastating as they could have been, it is important that states deploy the necessary measures to respond to both direct (when networks are directly targeted) and indirect (when damages are the consequences of attacks aimed at other targets) cyber-attacks. To this sense, the hybridization of conflicts, calls to the re-definitions of potential targets. When cyber-warfare is utilized, the military and civilian targets are oftentimes blurred as important but not military targets like corporations or hospitals arise.[15] The increased connectivity of the world makes the "attack surface" larger and the so called "critical infrastructures" are on the frontline. Given the fact that it is almost impossible to avoid being cyber-attacked, it is important to do everything possible to minimize potential damage if the attacker does get in.

Regarding the Russo-Ukrainian theater, it is probable that when military confrontations end, Russia will resort to the Cyber-Space to retaliate against the West for its involvement in the conflict. Before that happens, the west must be prepared to defend itself with efficacy.

Bibliography

Carmela Chirinos, "*Anonymous claims it hacked into Russian TVs and showed the true devastation of Putin's Ukraine invasion*", March 7, 2022, Retrieved from: https://fortune.com/2022/03/07/anonymous-claims-hack-of-russian-tvs-showing-putins-ukraine-invasion/

Steve Holland and James Pearson, "*US, UK: Russia responsible for cyberattack against Ukrainian banks*", February 18, 2022, Retrieved from: https://www.reuters.com/world/us-says-russia-was-responsible-cyberattack-against-ukrainian-banks-2022-02-18/

Dan Milmo, "*Anonymous: the hacker collective that has declared cyberwar on Russia*", February 27, 2022, Retrieved from: https://www.theguardian.com/world/2022/feb/27/anonymous-the-hacker-collective-that-has-declared-cyberwar-on-russia

Cristopher Del Fierro and John Dwyer, "*CaddyWiper: Third Wiper Malware Targeting Ukrainian Organizations*", March 15, 2022, Retrieved from: https://securityintelligence.com/posts/caddywiper-malware-targeting-ukrainian-organizations/

Hasherezade, Ankur Saini and Roberto Santos, "*HermeticWiper: A detailed analysis of the destructive malware that targeted Ukraine*", March 4, 2022, Retrieved from:

[15] https://hbr.org/2022/03/what-russias-ongoing-cyberattacks-in-ukraine-suggest-about-the-future-of-cyber-warfare

https://blog.malwarebytes.com/threat-intelligence/2022/03/hermeticwiper-a-detailed-analysis-of-the-destructive-malware-that-targeted-ukraine/

Peter Dickinson, "*Cyber partisans target Russian army in Belarus amid Ukraine war fears*", January 26, 2022, Retrieved from: https://www.atlanticcouncil.org/blogs/belarusalert/cyber-partisans-target-russian-army-in-belarus-amid-ukraine-war-fears/

Monica Buchanan Pitrelli, "*Anonymous declared a 'cyber war' against Russia. Here are the results*", March 16, 2022, Retrieved from: https://www.cnbc.com/2022/03/16/what-has-anonymous-done-to-russia-here-are-the-results-.html

Sergiu Gatlan, "*Russia shares list of 17,000 IPs allegedly DDoSing Russian orgs*", March 5, 2022, Retrieved from: https://www.bleepingcomputer.com/news/security/russia-shares-list-of-17-000-ips-allegedly-ddosing-russian-orgs/

James Pearson, "*Ukraine launches 'IT army,' takes aim at Russian cyberspace*", February 27, 2022, Retrieved from: https://www.reuters.com/world/europe/ukraine-launches-it-army-takes-aim-russian-cyberspace-2022-02-26/

Andrew Marino, "*Sandworm details the group behind the worst cyberattacks in history*", July 28, 2020, Retrieved from: https://www.theverge.com/21344961/andy-greenberg-interview-book-sandworm-cyber-war-wired-vergecast

Vish Gain, "*Ukraine cyberattacks: What you need to know*", February 24, 2022, Retrieved from: https://www.siliconrepublic.com/enterprise/ukraine-cyberattacks-ddos-hermetic-cyclops-russia-invasion

Sergiu Gatlan, "*Meta: Ukrainian officials, military targeted by Ghostwriter hackers*", February 28, 2022, Retrieved from: https://www.bleepingcomputer.com/news/security/meta-ukrainian-officials-military-targeted-by-ghostwriter-hackers/

Stuart Madnick, "*What Russia's Ongoing Cyberattacks in Ukraine Suggest About the Future of Cyber Warfare*", March 7, 2022, Retrieved from: https://hbr.org/2022/03/what-russias-ongoing-cyberattacks-in-ukraine-suggest-about-the-future-of-cyber-warfare

La Rivista semestrale *Sicurezza, Terrorismo e Società* intende la *Sicurezza* come una condizione che risulta dallo stabilizzarsi e dal mantenersi di misure proattive capaci di promuovere il benessere e la qualità della vita dei cittadini e la vitalità democratica delle istituzioni; affronta il fenomeno del *Terrorismo* come un processo complesso, di lungo periodo, che affonda le sue radici nelle dimensioni culturale, religiosa, politica ed economica che caratterizzano i sistemi sociali; propone alla *Società* – quella degli studiosi e degli operatori e quella ampia di cittadini e istituzioni – strumenti di comprensione, analisi e scenari di tali fenomeni e indirizzi di gestione delle crisi.

Sicurezza, Terrorismo e Società si avvale dei contributi di studiosi, policy maker, analisti, operatori della sicurezza e dei media interessati all'ambito della sicurezza, del terrorismo e del crisis management. Essa si rivolge a tutti coloro che operano in tali settori, volendo rappresentare un momento di confronto partecipativo e aperto al dibattito.

La rivista ospita contributi in più lingue, preferendo l'italiano e l'inglese, per ciascuno dei quali è pubblicato un Executive Summary in entrambe le lingue. La redazione sollecita particolarmente contributi interdisciplinari, commenti, analisi e ricerche attenti alle principali tendenze provenienti dal mondo delle pratiche.

Sicurezza, Terrorismo e Società è un semestrale che pubblica 2 numeri all'anno. Oltre ai due numeri programmati possono essere previsti e pubblicati numeri speciali.

EDUCatt - Ente per il Diritto allo Studio Universitario dell'Università Cattolica
Largo Gemelli 1, 20123 Milano - tel. 02.72342235 - fax 02.80.53.215
e-mail: editoriale.dsu@educatt.it (produzione) - librario.dsu@educatt.it (distribuzione)
redazione: redazione@itstime.it
web: www.sicurezzaterrorismosocieta.it
ISBN: 978-88-9335-956-6

Euro 20,00