Reassessing Russian Cyberwarfare and Information Warfare (2007-2022)

Andreis Gustavo Malta Purim [a], Bohdanna Duma [b]

[a] Institute of Computing, State University of Campinas in Campinas, São Paulo, Brazil. a213095@dac.unicamp.br

[b] Institute of Humanities and Social Sciences, Lviv Polytechnic National University, Lviv, Ukraine. bohdanna.duma.mv.2019@lpnu.ua

Abstract. Different from western military doctrine, the Russian concept of cyberwarfare is intrinsically related to Information Warfare. Instead of cyber operations being a complement to kinetic operations, such as disrupting enemy infrastructure, Russia defines them as a subset of information warfare, and thus, as a soft power non-kinetic way to influence other countries. This has caused western analysts to misinterpret the objective and successes of past Russian solely on tactical gains. This paper aims to explain the concept of cyber warfare from the Russian perspective, its evolutions from 2007 until 2022, and what are the perspectives for the future of cyberwarfare.

Keywords. Cybersecurity, Cyberwarfare, Cyber Attack, Information Warfare, Ukraine, Russia.

1. Introduction

On 23rd February 2022, the day before the beginning of Russian military operations, several Ukrainian government websites and banks were taken down by denial-of-service attacks [1]. At midnight, a hitherto unknown data-wiping malware was released in the country [2].

These attacks, together with previous incidents such as the hacking of Ukraine's power grid in 2016 [3] led many to believe the war in Ukraine would be a redefinition of hybrid and conventional warfare [4]. While the conflict is still unfolding, the use of cyberattacks has so far not given Russian forces the expected strategic and tactical advantage, which renewed debate on the role of cyberattacks in warfare [5]. Thus, the question remains: Why have Russian cyberattacks not been useful for achieving their military goals in Ukraine?

This paper aims to explain the concept of Russian cyberwarfare and its evolution from 2007 to 2022. Highlighting the idea of Information warfare and contrasting it with other countries, this study will propose why the Russian doctrine lacked tactical cyberwarfare planning for the invasion. It will also put forth some new metrics for evaluation of cyberoperations and ideas for future research, and a framework for responding to these attacks.

2. Methodology

2.1 Definitions of Cyberwarfare

Richard Clarke defines cyberwar as "actions by a nation-state to penetrate another nation's computers or networks for the purposes of causing damage or disruption" [6], and thus, is a subset of hybrid warfare, characterized by the use of non-state actors and non-military (non-kinetic) means to achieve military (kinetic) objectives [7]. Both definitions are debated among academics because of their ambiguity (either in the legal [8] or police-making [9] perspectives). There is also a distinction between cyberwarfare and cyberwar in scope and impact [10].

Every country has its own military doctrine, and thus, its own perception of cyberwarfare. Rarely is the word cyberwarfare (kibervoyna), rather, the concept inside the broader idea of information warfare (informatsionnaya voyna) [11]. The Military Doctrine of the Russian Federation (2010) states that a modern conflict features "prior implementation of measures of information warfare in order to achieve political objectives without the utilization of military force and, subsequently, in the interest of shaping a favorable response from the world community to the utilization of military force." [12].

Thus, Russian military thinking aggregates cyberattacks in the same field as disinformation and psychological operations, and thus takes a supporting role [11]. Also, Russian Cyberwarfare is also not a tactical, limited operation in wartime, but a continuous struggle for information control [13]. Therefore, Clarke's definition is still sufficiently valid, and this analysis will consider "cyberattack" a punctual action (i.e. the hacking of websites) component of a larger, time-limited "cyber operation" (i.e. the actions leading up to the invasion in 2022), which itself is a component of a continuous "cyberwarfare" – each operation will be separated by scope, target and evaluated.

2.2 Criteria of success of a cyber operation

J. A. Lewis measures the success of a cyberwarfare operation with two metrics: 1. Strategic Effect: the reduction of an opponent's will or capacity to resist; 2. Military effect: the degradation of an opponent's military capabilities, be they weapons, troops, or command and control [14]. The latter describes a western approach to cyberwarfare, while the former is more aligned with the Russian doctrine.

However, this division on the metric is unclear if attacks on civilian infrastructure are considered a strategic effect or a military one. Therefore, this study proposes redefining the metrics as 1. Information/Morale Effect: reduction of an opponent's will or capacity to resist, be it from a long-term shift in public opinion or short-term 'shock and awe' and 2. Infrastructural effect: degradation of the opponent's physical or digital infrastructure, be they civilian or military – also takes into account cyberespionage or the threat to another country's system by unauthorized access.

2.3 Allegations of State Involvement.

Cyberattacks are generally conducted by anonymous individual or groups with untraceable origins, thus creating a legal gray zone where countries have plausible deniability, as these actors can be either state officials, state-sponsored groups, or acting on their own for the advancement of their country. [8]

While minor incidents such as DDoS attacks are easily reproducible by individuals, complex software such as Stuxnet can only be developed with resources from nation-states. [8] "Fancy Bear" and "Sandworm", two cyberespionage groups, have been identified as units within the GRU (Russia's Main Intelligence Directorate), with 6 Russian operatives being indicted by the US Department of Justice in 2020 [15].

"Fancy Bear", for example, is classified as an advanced persistent threat, whose operatives are Russian speakers and operate in a timezone consistent with Moscow and St. Petersburg, finally, their goals are focused on collecting intelligence (as opposed to economic gain) in the post-soviet sphere that would be useful for governments, especially Russia [16].

3. Evolution of Russian Cyberwarfare

3.1 Post-soviet sphere from 2007

During April and May 2007, Estonian websites were attacked by denial-of-service attacks in what is considered "the first large-scale coordinated use of cyber by Russia to affect a strategic outcome in a neighboring state" and were followed by Russia demanding to freeze diplomatic ties and impose sanctions on Estonia. The operation started only hours after the Estonian government decided to move a Soviet statue from its location [11].

Similar attacks took place in Lithuania in June 2008 and Kyrgyzstan in 2009 with DoS attacks in response to opposition to the Russian government [17]. Similar, low-intensity operations continued throughout the decade, with the last notable example was an attack on the Latvian Election Commission in 2018 [18].

Analysts consider the infrastructural effect was minimal, as relations between the countries normalized and websites were restored [14]. But in the information field, Russia demonstrated that it could interfere and coerce neighboring countries without triggering an international response, with the Estonian Minister of Defense declaring "the aim (...) was to destabilize Estonian society, creating anxiety among people that nothing is functioning, the services are not operable, this was clearly psychological terror in a way" [11]. This pattern will continue to be fundamental to Russian cyberwarfare thinking up to 2022.

3.2 Russo-Georgian War (2008)

The cyber-attacks in Georgia started on July 20, 2008 - three weeks before the Russian invasion - being the first time attacks in the cybersphere were coordinated and coincided with direct armed hostilities. These attacks included the redirection of Georgian servers to other countries, the creation of fake news, a significant slowdown in access to government sites [17][16]. In matters of impact, however, there is no evidence suggesting permanent infrastructural damage by the attacks or a decrease in Georgian morale.

3.3 Ukraine (2014-2022)

The first attacks on the information system of private and state institutions in Ukraine were recorded during the protests in 2013 and from 2014 were often coincidental to kinetic actions in Crimea and Eastern Ukraine [5]. Many of the low-scale actions are relayed on DDoS attacks, which are similar to previous actions and do not cause much damage. Some sophisticated Russian operations must be highlighted:

First, Operation Snake (2013-2014), a surge of detected cases of infection of information systems of Ukraine with a computer worm with rootkit, nicknamed “the snake”. [19] Secondly. CyberBerkut, a pro-russian group, togheter with Fancy Bear, conducted several operations hacking and exposing private documents about Ukranian officials. [20]

Then, from 2016. “Fancy Bear” developed Xagent, a malware, which stole information from SMS content, call log, and the geolocation of the infected device. It was also claimed that it could be used to hack Ukranian’s D-30 Howitzer artillery [21] and “Sandworm” developed Petya, a family of ransomware encrypting malware developed by the “Sandworm” group. Later, new variants such as NotPetya, BadRabbit and WannaCry are belived to be derived from Petya. [22]

These refined attacks show the level of resources and capabilities of the Russian Government. While previous attacks in Georgia and Estonia were mainly for morale purposes, the attacks on Ukraine show infrastructural aims, such as collecting the location of devices or wiping and encryption of government data. This is further reinforced by the cyberattacks on Energy Companies in Ukraine (2015-2017), which show a Russian focus on damaging energy infrastructure, further reinforcing European dependency on Russian oil and gas [3].

3.4 Ukraine (2022)

On January 14, 2022, about 22 government agencies and 70 Ukrainian websites were hacked. On February 23, regular attacks were made on banking and government sites with the HermeticWiper virus, a new malware detected by ESET. This virus file system was named with taunts against the US government and President Biden [23].

At midnight on the 24th, the Kyiv Regional State Administration was attacked and numerous e-mails with pishing links were sent to Ukrainian servicemen. This attack was identified by Google to be originated from “Fancy Bear”. [24]

Furthermore, SMS were sent to the phones of Ukrainian citizens falsely relating that certain regions or cities had already been invaded, causing panic. This indicates that some breach of private or government data regarding private phone numbers was also executed. [25]

However, these attacks failed to give any advantage to the Russian ground forces. The reasons for such will be discussed in the next topic.

4. Discussion

4.1 Doctrines from other Countries

While the Russian doctrine is focused on continuous information warfare, USA and Israeli doctrines fall into the western definition of tactical, limited operations with a clear goal integrated in combined arms warfare [13] Israel is an example of cyberwarfare doctrine fully integrated in combined arms warfare, with the Stuxnet virus targeting enemy infrastructure [28].

Meanwhile, China has had a similar view to Russia on Information Warfare, with recent developments on the concept of cyberwarfare [29]. This idiosyncrasy should be noted when analyzing or preparing cyberoperations.

4.2 A Synthesis of Russian Cyberwarfare

As explained in the methodology chapter, Russian Military Doctrine regards cyberwarfare as a tool for information control, not part of combined arms warfare [13]. It is clear that Russia has the technical capabilities and resources of creating sophisticated malware, as evidenced by the operations in Ukraine (2014-2022) [17]. However, regarding back the Russian Military Doctrine document emited by President Vladmir Putin in 2010, the focus is of informational warfare “implementation of measures of information warfare in order to achieve political objectives without the utilization of military force” [12].

This explains why Russian ground forces have failed to capitalize on hacker attacks as a tactical advantage in warfare in Georgia and Ukraine. Russian focus continues to be in propaganda and pression (Information and Morale effects) on the population. Moreover, the coercive diplomacy executed by Russia has also failed in both cases [26].

4.3 What happened on 24th February?

Other than the HermeticWiper, no other malware has been reported in Ukraine during the invasion. As stated before, Russia differs from western countries in its doctrine. The planning for the invasion of 2022 appears to have relied on initial shock-and-awe and the assumption that Ukrainian defenses would be disorganized and falter quickly [27]. Thus, Russian Command may have been confident in its kinetic capabilities and disregarded the need for cyberwarfare [5]. The pishing links and SMSs, together with propaganda, would have been sufficient to disorganize Ukrainian defenses.

Meanwhile, Western companies and ‘Hacktivists’ helped create a Ukrainian ‘IT’ army to counter Russian attacks. Furthermore, the costs in human capital and investments may have been considered too expensive for a campaign Russia thought would be easily won by conventional means [5].

4.4 Quantitative Research

Cyberwarfare data for quantitative research is often hard to find. Adebiaye et al. (2016) already hinted at using surveys on victims [29] while Gazula (2017) rated cyberoperations discretely using metadata [30], sources from the following years in Ukraine should provide ample space for studies. A possible innovation would be statistical approach combining metadata as dummy variables and cost (in equipment or manpower) and number of people affected to create a continuous rating of “impact” of cyberoperations.

5. Conclusions

5.1 Cyber: Bad doctrine or incapacity?

Specialists such as Valeriano et al. predicted correctly that Ukraine would not be a new era in cyberwarfare, and that these operations are incapable of generating impact on themselves [5], This falls in line with Ashraf's 'skeptic' concept [8]. However, Russian coercive diplomacy [26] and military planning [27] have also shown to be badly designed, therefore failure in the Russian application should not discredit the concept as a whole, as Israel proved that it can achieve significant results if applied correctly [28]. Why Isreal succeeded where Russia failed is a topic for future research.

5.2 New Concepts and Response

This study used Richard Clarke's definition of cyberwar (as an equivalent to cyberwarfare) for simplicity, but concepts such as 'cyber incidents' should be considered more precise in future research [26][18]. In fact, a majority of articles on cyberwar fail to give an explicit definition [8], highlighting the need for a reassessment of the concepts – such as this paper.

Meanwhile, this paper has also proposed 2 new qualitative metrics adapted from J.A. Lewis [14] and ideas for quantitative analysis for future research.

Finally, Ukraine has shown that a 'hacktivist' IT army and companies were capable of neutralizing these threats efficiently (HermeticWiper was detected the day it was released [23]), countries in the EU – such as the Baltic States - should take these examples in creating forums, groups and networks for response in these cases.

6. References

[1] Feiner, L. Cyberattack hits Ukrainian banks and government websites. CNBC [online]. 2022 Feb 23 [cited 4 Apr 2022]. Available from: https://www.cnbc.com/2022/02/23/cyberattack-hits-ukrainian-banks-and-government-websites.html

[2] Tidy, J. Ukraine crisis: 'Wiper' discovered in latest cyber-attacks. BBC [online]. 2022 Feb 24 [cited 2022 Apr 4]. Available from: https://www.bbc.com/news/technology-60500618

[3] Zetter, K. Inside the Cunning, Unprecedented Hack of Ukraine's Power Grid. Wired [online]. 2022 Mar 3 [cited 4 Apr 2022]. Available from: https://www.wired.com/2016/03/inside-cunning-unprecedented-hack-ukraines-power-grid/

[4] Miller, M. Russian invasion of Ukraine could redefine cyber warfare. Politico [online]. 2022 Jan 28 [cited 4 Apr 2022]. Available from: https://www.politico.com/news/2022/01/28/russia-cyber-army-ukraine-00003051

[5] Lonergan E, Lonergan S, Valeriano B, Jensen B. Putin's invasion of Ukraine didn't rely on cyberwarfare. Here's why. The Washington Post [online]. 2022 Mar 7 [cited 4 Apr 2022]. Available from: https://www.washingtonpost.com/politics/2022/03/07/putins-invasion-ukraine-didnt-rely-cyber-warfare-heres-why/

[6] Clarke R, Knake R. Cyber War: The Next Threat to National Security and What to Do About It, Reprint edition. New York: Ecco; 2012

[7] Fleming B. The Hybrid Threat Concept: Contemporary War, Military Planning and the Advent of Unrestricted Operational Art [Internet]. Fort Leavenworth (US): Defense Technical Information Center; 2011 [cited 4 Apr 2022]. Available from: https://apps.dtic.mil/sti/citations/ADA545789

[8] Ashraf C. 2021. Defining cyberwar: towards a definitional framework. Defense & Security Analysis. 2021 Aug 6; 37(3):274-294.

[9] Bērziņš J. (2020) The Theory and Practice of New Generation Warfare: The Case of Ukraine and Syria. The Journal of Slavic Military Studies. 2020 Dec 14;33(3): 355-380.

[10] Green J, editor. Cyber Warfare: A Multidisciplinary Analysis. London (GB): Routledge; 2015

[11] Conell M, Vogler S. Russia's Approach to Cyber Warfare [Internet]. Arlington (US): Office of the Chief of Naval Operation; 2017 [cited 4 Apr 2022]. Available from: https://apps.dtic.mil/sti/pdfs/AD1032208.pdf

[12] The Military Doctrine of the Russian Federation. Moscow (RU): Russian Federantion Presidential Edict; 2010 [cited 4 Apr 2022]. Available from: https://carnegieendowment.org/files/2010russia_military_doctrine.pdf

[13] Giles K, Seaboyer A. The Russian Information Warfare Construct [Internet]. Kingston (CAN): Royal Military College of Canada; 2019 [cited 4 Apr 2022]. Available from: https://cradpdf.drdc-rddc.gc.ca/PDFS/unc341/p811007_A1b.pdf

[14] Geers K, Lewis JA. Cyber War in Perspective: Russian Aggression against Ukraine [Internet]. Tallinn (ES): NATO CCD COE; 2015. Chapter 4, 'Compelling Opponents to Our Will': The Role of Cyber Warfare in Ukraine. [cited 4 Apr 2022].

Available from: https://www.usna.edu/CyberDept/_files/documents/CyberWarinPerspective_Lewis_04.pdf

[15] Six Russian GRU Officers Charged in Connection with Worldwide Deployment of Destructive Malware and Other Disruptive Actions in Cyberspace [Internet]. Washington (US): U.S. Department of Justice; 2020 [cited 4 Apr 2022]. Available from: https://www.justice.gov/opa/pr/six-russian-gru-officers-charged-connection-worldwide-deployment-destructive-malware-and

[16] APT28: At the Center of the Storm [Internet]. Milpitas (US): FireEye; 2017 [cited 4 Apr 2022]. Available from: https://www.mandiant.com/resources/report-apt28-a-window-into-russias-cyber-espionage-operations

[17] Ashmore W. Impact of Alleged Russian Cyber Attacks [Internet]. Fort Leavenworth (US): School of Advanced Military Studies; 2009 [cited 4 Apr 2022]. Available from: https://apps.dtic.mil/sti/pdfs/ADA504991.pdf

[18] Viksnins K. Cyberwarfare in Latvia: A Call for New Cyberwarfare Terminology. FPRI [online]. 2022 Jun 23 [cited 4 Apr 2022]. Available from: https://www.fpri.org/article/2020/06/cyberwarfare-in-latvia-a-call-for-new-cyberwarfare-terminology/

[19] Snake Cyber-espionage Campaign Targetting Ukraine is Linked to Russia. InfoSecurity [online]. 2014 Mar 11 [cited 4 Apr 2022]. Available from: https://www.infosecurity-magazine.com/news/snake-cyber-espionage-campaign-targetting-ukraine/

[20] Joselow G. Election Cyberattacks: Pro-Russia Hackers Have Been Accused in Past. NBC [online]. 2016 Nov 3 [cited 4 Apr 2022]. Available from: https://www.nbcnews.com/mach/technology/election-cyberattacks-pro-russia-hackers-have-been-accused-past-n673246

[21] Meyers A. Danger Close: Fancy Bear Tracking of Ukrainian Field Artillery Units. Crowdstrike [online]. 2016 Dec 22 [cited 4 Apr 2022]. Available from: https://www.crowdstrike.com/blog/danger-close-fancy-bear-tracking-ukrainian-field-artillery-units/

[22] BadRabbit: a closer look at the new version of Petya/NotPetya. MalwareBytes [Online]. 2017 Oct 24. [cited 4 Apr 2022]. Available From: https://blog.malwarebytes.com/threat-analysis/2017/10/badrabbit-closer-look-new-version-petyanotpetya/

[23] Guerrero-Saade JA. HermeticWiper | New Destructive Malware Used In Cyber Attacks on Ukraine. SentinelLabs [online]. 2022 Feb 23 [cited 4 Apr 2022]. Available from: https://www.sentinelone.com/labs/hermetic-wiper-ukraine-under-attack/

[24] Huntley S. An update on the threat landscape. 2022 Mar 07. In: Updates from Threat Analysis Group (TAG) [Internet]. Mountain View (US): Google. Available from: https://blog.google/threat-analysis-group/

[25] Shannon Vavra. Disturbing Mass Text Operation Terrorizes Ukraine as Russian Troops Move In. Daily Beast [online]. 2022 Feb 23 [cited 4 Apr 2022]. Available from: https://www.thedailybeast.com/cyberattacks-hit-websites-and-psy-ops-sms-messages-targeting-ukrainians-ramp-up-as-russia-moves-into-ukraine?ref=scroll

[26] Karlsson E. Cyberwar – A 21st century Maskirovka? A qualitative analysis over Russian coercive diplomacy through cyberattacks in Georgia and Ukraine [bachelor's thesis on the internet]. Uppsala (SW): Uppsala University; 2021 [cited 4 Apr 2022]. Available from: https://www.diva-portal.org/smash/get/diva2:1627644/FULLTEXT01.pdf

[27] Beauchamp Z. Why the first few days of war in Ukraine went badly for Russia. Vox [online]. 2022 Feb 28 [cited 4 Apr 2022]. Available from: https://www.vox.com/22954833/russia-ukraine-invasion-strategy-putin-kyiv

[28] Baram G. Israeli defense in the age of cyber war. Middle East Quarterly. 2017 Jan;24(1):1-10

[29] Fritz J. China's development of cyber warfare doctrine: a conceptual and historical investigation [dissertation on the Internet]. Gold Coast (AU): Bond University; 2015 [cited 4 Apr 2022]. Available from: https://pure.bond.edu.au/ws/portalfiles/portal/36191330/Jason_Fritz_Thesis.pdf

[29] Adebiaye R, Alryalat H, Owusu T. Perspectives for Cyber-Deterrence: A Quantitative Analysis of Cyber Threats and Attacks on Consumers. Int. j. innov. res. sci. eng. technol. 2016 Jul;5(7).

[30] Gazula M. Cyber Warfare Conflict Analysis and Case Studies [master's thesis on the Internet]. Boston (US): Massachusetts Institute of Technology; 2017 Jun. Available from: https://cams.mit.edu/wp-content/uploads/2017-10.pdf