INTERNATIONAL CONFERENCE RCIC'22
Redefining Community in Intercultural Context
Braşov, 5-7 May 2022

DIGITAL GOVERNANCE IN NATIONAL SECURITY THREAT MANAGEMENT

Claudia LASCATEU*

*Expert, Romanian Intelligence Service, Bucharest, Romania

Motto

"However critical may be the situation and circumstances in which you find yourself, do not despair. It is on occasions when everything is to be feared that nothing is to be feared. It is when one is surrounded by all dangers that one need not fear any. It is when one is without any resources that one must count on them all. It is when one is surprised that one must surprise the enemy himself."
Sun Tzu, *The art of war*

Abstract: *Digital public policy and national security threat management are shifting at a pace that is hardly ever synchronized. Both areas of expertise require different sets of incentives to move in one direction, nonetheless for implementing successful digital transformation strategies it is required to adapt to a common responsible approach of the toolkit that new technology offers in national security threat prevention. This study is set to outline that digital governance in an intelligence service that also assumes a digital presence is mainly represented by the framework of responsibility where role definition and decision-making are put into action. Therefore, digital governance in a national security structure means it is invested with powers by the law but also can delegate specific executive authority given the plethora of scenarios that can occur in order to efficiently prevent incidents that can potentially disrupt the status quo. Hence, it will firstly be outlined what security stands for today in a syncretic analysis that binds the principles of good governance and human rights using the filter of innovation in technology. Secondly, the paper will navigate through digital strategy, digital policy and digital standards in order to build the importance of the role of managing security disruptions that are considered possible threats to national security. A digital maturity may have been reached in national security organizationally-wise, but threats developed in the processes of future technologies must be the subject of the discussion to strengthen the wellbeing of our society.*

Keywords*: digital policy; national security threat management; digital strategy; digital standards*

1. INTRODUCTION

Threats bear the force to change security landscape but today's intelligence organizations are absorbing reforms driven by the demands the digital society requests, a society that wants to no longer be divided by territory, that is prone to be consumed in media extravaganza of scandal, facing all sorts of emotional extremes. Like the logic of commodities prevails over competitive ambitions of merchants, or the logic of war determines frequent modification of weapons, or the logic of spectacle needs a diversity of media exposure, the national security logic commands digital proficiency in all matters, including digital threat management.

The change that we have been seeing the past 10 years has been of importance both as a diversification of disruptions that appear to act as incentives to further the digital expertise of state backed organizations, but also as an intrinsic rearrangement of frameworks to meet the competition of outside players.

2. THREATS IN A DIGITAL SOCIETY

To give technology authority is to recognize it has merged into our society and stands to empower media. Then, if technology plays such an important part is it time to say that when corporate interests come to dominate media it changes the way we perceive historical truth? It is not always the case, but incentives to determine certain narratives have been observed. It presents a natural attraction to some people to gain absolute control over the information that reaches society, to model the knowledge voting people have. To build the present-day to your own liking in people's minds sounds quite tempting, a godlike tool that completes the framework of a closed society, a captive one.

To live in complete ignorance of what the government is actually conducting will always make it easier to forget when it will come out, that's why the most important facts are the ones that are mostly hidden, covered in complete secrecy - a generalized secrecy that stays behind the entertainment provided by the controlled media.

In a state-led media existence, there is no need for feedback, no need for critical thinking and apparently no sanctions. The narratives gain authority and society validates them, in its ignorance. It comes easily to become a speechless individual under such long lasting circumstances, and that's how one systematically destroys public opinion. This is the case of authoritarian states that intend to preserve power and to design an alternate history, above the law, that matches their leader's vision. What you can equally find in democratic states is the toolkit offered by new technologies.

Why is it that we find it so comforting to live in a digital society one may ask? Maybe because values and morals seem to dissipate in digital space and makes it easier to act impersonally, to spend time in such a place where no moral compass applies, so there would be no sanctions. It feels easier without having a referee. Luckily, it's only the perception users get. Of course, in the transition to digital life all the vulnerabilities that come with the territory apply. When those vulnerabilities are explored to an extent that can create serious damage, a disruption to normal life, then we can evaluate the level of danger that the emerged threat is capable of delivering on a day-to-day basis, but most importantly in times of armed conflict.

We must acknowledge that the vulnerabilities that arise in times of duress may come as an advantage for the aggressor, take for instance the outage of ViaSat[1] the day the Russian invasion started that affected the Ukrainian armed forces, police and intelligence service (Rid, 2022), that is why an effective threat management has to function properly - which goes from identifying the threat, to damage control and counteracting.

Are these measures lawless one might wonder? As long as we have a framework for the development of the toolset to actively safeguard the security, and within this framework we can clearly see the national strategy, the policy adopted and the standards employed in dealing with digital threats, the spirit of the law speaks for itself.

Besides the cyberattacks that can be distinguished by the technological factor, anonymity of the actors and tangible disruptions that we can equivalate to basic covert operations, we must equally pay attention to the increased disinformation operations that originate in state-funded media outlets of authoritarian states and their proxy social media channels that affect the mindsets of millions of followers world-wide.

Months before the start of the Russian war with Ukraine in 24th February 2022, there was a historical effort in the amount of information that was declassified to actively act as both early warning to international community (London, 2022) and deterrent to the aggressor state (Elliott, 2022). That is the time timeframe when we could consider was the beginning of a media frenzy (Dorfman, 2022) that should have been considered as legitimate warning of a full-scale armed conflict in the days that followed. First main disclosure came in December 2021 and cautioned about the amassed Russian troops on the eastern Ukrainian border that are ready to start an offensive in early 2022 (Harris, 2021), publishing satellite pictures of the troops estimated at 175,000 and 4 geographical locations of the multi-front offensive.

Meanwhile the state-funded Russian media and their proxies started pushing the narrative that NATO and the West control the Ukrainian government against the interests of the Ukrainian people, a theme that has been revisited since the illegal Russian occupation of Crimea in 2014 and supported the separatist movement in Donbas region. Officially the response Putin offered was that the NATO exercises in the Black Sea region alongside the Romanian and Polish anti-missile American systems are threats to Moscow.

In January, U.K. stated that the Russian plan is to forcefully remove Ukrainian president Volodymyr Zelensky to be replaced with a pro-Kremlin leader, possibly Viktor Medvedchuk, a close family friend of Putin (Shuster, 2022). The U.S. warned also about Russia sending saboteurs to generate a formal reason for the war (Plett-Usher, 2022). The same day, Ukraine calls out on Russia cyberattack on almost 70 of official sites that went down with an anti-Ukrainian government message (Tidy, 2022).

The beginning of February U.S. warned about an imminent Russian attack on Ukraine and urged its citizens to leave the country. February 21st Kremlin recognizes the independence of the 2 self-proclaimed separatist regions Donetsk and Luhansk to build a legitimate pretext to proceed with the invasion. On February 23rd and 24th Russian launched 3 wiper cyberattacks that hit Ukrainian systems just hours before the airstrikes started (Guerrero-Saade, 2022).

Given the public's saturation with alarming news, disinformation accusations from all the sides

[1] A highspeed satellite broadband operator

implicated, the possibility of an actual Russian invasion has been dismissed in the mainstream public opinion until it actually happened. Few had started packing to take western refuge when clear signs of an imminent armed conflict were there - Russian ethnics started burning documents in the streets, Russian diplomats and nationals left Ukraine a couple days before the Russian air strikes started to hit Ukrainian targets.

Two days after the war against Ukraine started the claims presented officially in National Security Council by Putin on national television were that Ukraine is committing genocide against Russian ethnics and is led by Nazi ideology and drug addicts, justifying the special military operation in progress. The days that followed a movement to stop the access of Russian backed media outlets on European and American public appeared, so by the beginning of March the ban was in place (Kayali, 2022), but what is unprecedented is that Google's YouTube streaming service and other social media giants like Meta followed. Moldova also issued an order to ban Sputnik and Gagauznet media-outlets. This straight forward movement against disinformation complements the unprecedented economic sanctions put into place by the U.S. and the E.U.

Given the growing economic sanctions on Russia and the invasion that is moving slower than anticipated, Kremlin has made sure that nuclear weapons come back into people's mindsets reminding of Cold War era fear of mutual destruction, cautioning against Western military involvement in Ukraine and condemning the military technology support offered by NATO allies calling them unfriendly states and saying that foreign military support offered to Ukraine is considered a legitimate target. Also, Putin asserted that unfriendly states will have to use Russian currency to pay for oil and gas contracts given that the rouble plummeted due to sanctions on Russia National Bank.

Official declarations regarding nuclear missiles and reports of Russian military offensive on Chernobyl generating a fire close to the conservation silo has successfully raised once again fears of radiation and remembering the '86 nuclear catastrophe Romanian people already anxious about the war closing to borders have started to pile up reserves of potassium iodine in hope to have a chance to survive such an event. Alarmist channels that fed Covid-19 conspiracy theories turned into military analysts launching pro-Russian propaganda feeding most popular attractive narratives that prove to be only myths about the war in Ukraine, but their success on Romanian public is merely marginal, being met by popular detestation fueled by tragic memories of past soviet military inhumane treatment of civilians and forced deportations Romanian people suffered.

Mainstream media started to present the steps to be taken in such an event, to popularize the official locations of anti-atomic bunkers, to show that authorities renew the national reserve of medication and equipment.

Further, mid-March the focus of Kremlin disinformation shifted towards Russian population reviving an older narrative of U.S. operated biochemical laboratories in Ukraine (Price, 2022) that are the source of pathogens like Covid-19 (Lee, 2022). The Kremlin also claimed that the takeover of Chernobyl former nuclear power plant was to prevent the creation of a Ukrainian nuclear dirty-bomb (Mallard, 2022) and the military invasion of Ukraine is a peacekeeping operation. Kremlin's propaganda and disinformation have been systematically dismantled by immediate response and effort by European and U.S. agencies that also presented the public the unnecessary massive civilian targeting practiced by the Russian Army on Ukrainian territory.

Even though considered a massive win in information war, the following days other propaganda and disinformation tactics surfaced that evade Kremlin association and the restrictions but come under the anonymity umbrella offered by other social media networks such as Telegram (Scott, 2022). TikTok algorithm does not filter content by truthfulness so it effectively has become a place for active measures for both sides of the Russian – Ukrainian conflict (Hern, 2022).

Active measures step up when transparently Kremlin funded media-outlets like RT - Russia Today, Sputnik and TASS are taken out of the main reach of western population – this is where proxy come into play: troll farms, news websites, academic websites, publishing research foundations with ties to Russia's Foreign Intelligence Service (SVR) like The Strategic Culture Foundation, Global Research, New Eastern Outlook, News Front, Southfront, Katehon, Geopolitica.ru (State, 2020). Dealing with this sort of disruption in a form that was not presenting new attributes, but had a baffling effect on neighboring countries, as for the scale and brutality the aggression developed throughout the days, puts to a test even the most seasoned national security organizations that implement common digital disruption strategies. It is based on a wholesome understanding of media platforms that once again proves to be an effective tool.

Adapting to the challenges that occur every hour fueled by an armed conflict that uses all that

technology can offer to obtain an advantage on the field, displays how an effective digital policy in threat prevention works.

Another important part of the process is effectively implementing digital standards, that are identifying disinformation models, trending patterns in media multiplier effect and creation of a fact-based adequate response.

3. CONCLUSIONS

Having a flexible analysis on how media ecosystem evolves in this European war scenario plays a crucial part in threat prevention and must take into account what are the leading shifts that form new disinformation tools and what are the effects of how the western media is tackling the challenge of scaling down by taking action against fake-news at the cost of profits.

In the digital governance of national security threat management, we reach a milestone where we surpass ideologies but use their influences to strategize in order to have efficient souple operations, integrated systems to aid decision-making. We must continue the incessant work for defining and identifying types of threats that use system vulnerabilities that have the potential to cause disruption of our status quo in order to find remedies in due time. Also, we must educate the public to correctly identify disinformation since most of times it plays to our fears and anxieties feeding false narratives to gain control over the mindset of the population. The possibility to falsify reality to a degree that history becomes flexible and convenient to those that control the information is a greater threat on the long-term than any damage that a cyberattack can cause.

BIBLIOGRAPHY

1. Dorfman, Z. (2022, February 20). In new front of information war US repeatedly declassifies intelligence on Ukraine and Russia. *Yahoo News* [online]. Available: https://news.yahoo. com/in-new-front-of-information-war-us-repeatedly-declassifies-intelligence-on-ukraine-and-russia-224649617.html?guccounter=1&guce_referrer=aHR0cHM6Ly93d3cuZ29vZ2xlLmNvbS8&guce_referrer_sig=AQAAALdV0tVF-ZrkKpoUJOJhV4LCG2KepeO1jeOQz_ tM5x [Accessed March 2022].
2. Elliott, P. (2022, February 16). Why the CIA Director Is Declassifying Material on Russia's Ukraine Plot. *Time* [online]. Available: https://time.com/6148791/william-burns-cia-russia-declassify/ [Accessed March 2022].
3. Guerrero-Saade, J. A. (2022, February 28) HermeticWiper | New Destructive Malware Used in Cyber Attacks on Ukraine. *Sentinel Labs* [online]. Available: https://www. sentinelone.com/labs/hermetic-wiper-ukraine-under-attack/ [Accessed March 2022].
4. Harris, S. (2021, December 3). Russia planning massive military offensive against Ukraine involving 175,000 troops, U.S. intelligence warns. *The Washington Post* [online]. Available: https://www.washingtonpost.com/ national-security/russia-ukraine-invasion/2021/ 12/03/98a3760e-546b-11ec-8769-2f4ecdf7a2ad _story.html [Accessed March 2022].
5. Hern, A. (2022, March 21). TikTok algorithm directs users to fake news about Ukraine war study says. *The Guardian* [online]. Available: https://www.theguardian.com/technology/2022/mar/21/tiktok-algorithm-directs-users-to-fake-news-about-ukraine-war-study-says [Accessed March 2022].
6. Kayali, L. (2022, February 27). Ursula von der Leyen announces RT Sputnik ban. *Politico* [online]. Available: https://www.politico.eu/ article/ursula-von-der-leyen-announces-rt-sputnik-ban/ [Accessed March 2022].
7. Lee, E. (2022, February 25). Fact Check Claim US Biolabs Ukraine Disinformation. *USAToday* [online]. Available: https://eu.usatoday.com/ story/news/factcheck/2022/02/25/fact-check-claim-us-biolabs-ukraine-disinformation/69379 23001/ [Accessed March 2022].
8. London, D. (2022, February 15). To reveal or not reveal. *Foreign Affairs* [online]. Available: https://www.foreignaffairs.com/articles/ukraine/2022-02-15/reveal-or-not-reveal [Accessed March 2022].
9. Mallard, W. (2022, March 06). Russia Without Evidence Says Ukraine Making Nuclear Dirty Bomb. *Reuters* [online]. Available: https:// www.reuters.com/world/europe/russia-without-evidence-says-ukraine-making-nuclear-dirty-bomb-2022-03-06/ [Accessed March 2022].
10. Plett-Usher, B. (2022, January 14). Russia-Ukraine: US warns of 'false-flag' operation. *BBC* [online]. Available: https://www.bbc.com/ news/world-europe-59998988 [Accessed March 2022].
11. Price, N. (2022, March 09). The Kremlin's allegations of chemical and biological weapons laboratories in Ukraine. *U.S. Department of State* [online]. Available: https://www.state. gov/the-kremlins-allegations-of-chemical-and-biological-weapons-laboratories-in-ukraine/ [Accessed March 2022].
12. Rid, T. (2022, March 18). Why You Haven't Heard About the Secret Cyberwar in Ukraine. *New York Times* [online]. Available: https:// www.nytimes.com/2022/03/18/opinion/cyberwar-ukraine-russia.html [Accessed March 2022].
13. Scott, M. (2022, March 10). As war in Ukraine evolves, so do disinformation tactics. *Politico* [online]. Available: https://www.politico.eu/ article/ukraine-

russia-disinformation-propaganda/ [Accessed March 2022].
14. Shuster, S. (2022, February 02). The Untold Story of the Ukraine Crisis. *Time* [online]. Available: https://time.com/6144109/russia-ukraine-vladimir-putin-viktor-medvedchuk/ [Accessed March 2022].
15. Tidy, J. (2022, January 14). Ukraine cyber-attack: Russia to blame for hack, says Kyiv. *BBC* [online]. Available: https://www.bbc.com/ news/world-europe-59992531 [Accessed March 2022].
16. U.S. Department of State (2020, April 08). Disinformation and Propaganda Ecosystem 2020. *U.S. Department of State* [online]. Available: https://www.state.gov/wp-content/ uploads/2020/08/Pillars-of-Russia%E2%80%9 9s-Disinformation-and-Propaganda-Ecosystem_08-04-20.pdf [Accessed March 2022].