European Union Institute for Security Studies

BRIEF / 19
Nov 2023

FROM CYBER TO HEARTS AND MINDS

Cyber operations and the battle for global influence

The EUISS is an agency of the European Union

CONFLICT SERIES

by

Viola Fee Dreikhausen
Associate Analyst, EUISS

Andrea Salvi
Senior Analyst, EUISS

On 5 October 2023, a group of pro-Russian hackers announced in a Telegram post that it was targeting the Australian Home Affairs department with a distributed denial-of-service (DDoS) attack. The post cited Australia's decision 'to keep up with the global Russophobic trend' and deliver the 'Slinger "drone killer system" to Kyiv' as the motive for the attack[1].

While a government spokesperson confirmed that the Home Affairs website was taken down for about five hours between 10pm and 3am AEDT, the hackers did not access any data. Notwithstanding the comparatively limited extent of the inflicted damage, the incident reveals the true nature of low-intensity cyberattacks. Such attacks take place in a context where perception, posturing and projections are key. By using cyber vectors and targeting information systems, 'hearts and minds' can be directly influenced. In this Brief, we focus on a set of operations that sit at the intersection of two distinct spheres – the cyber and human domains.

Cyber influence operations (CIOs) are a subset of influence operations that combine the use of force on cyber infrastructure with a broader strategy of interference in the human domain, that is, the dimension

Summary

- Cyber influence operations use cyber vectors to target the human domain – the dimension of conflict that centres on competing actors' efforts to influence human perception in their pursuit of strategic objectives.
- The novelty of cyber influence operations resides in their highly disruptive nature, targeting both cyber-digital infrastructures and societal resilience/cohesion.
- Cyber influence operations have been widely conducted in the war in Ukraine. Russia's approach has been multifaceted, involving activities that target the cyber and human domains in support of its broader strategic goals.
- Current capabilities are tilted towards reacting to cyberattacks. Accordingly, there is a need for integrated approaches that address the intricate landscape of influence and perception in the cyber domain.

Incident types as coded by EuRepoC

Disruptions
refer to operations that aim to violate the availability of digital information in a temporary or permanent way. Disruptions include DDoS, defacements, and wiper malware. Examples include the self-attributed DDoS attacks of the hacking group known as KillNet against NATO websites in February 2023 .

Doxing
refers to the willing exfiltration and divulgation of information obtained through hacking activities. It is also known as 'hack-and-leak'.
Doxxing has been used widely both in peace and war time operations. Examples include hacking and leakage of private information from U.S. soldiers in 2015 by a pro-Islamic Group . It has been used extensively in Russia's war of aggression in Ukraine .

Hijacking
refers to cyber incidents that aim to gain control of a computer or computer network.
Hijacking allows perpetrators to gain control of and compromise networks and systems connected to them. Examples include the actions of the allegedly Iranian state-sponsored hacking group Peach Sandstorm that, in February 2023, gained access to various organisations globally, including in the satellite and defence sectors.

Data: EUREPOC , 2023

of conflict and warfare that centres on competing actors' efforts to influence human perception in their pursuit of strategic objectives. Accordingly, CIOs draw on cyber vectors to shape the attitudes and actions of adversaries and non-aligned parties. In case of open conflict, this may have important implications on the balance of power in a warzone. For example, in 2023 Russia reportedly launched between 10 and 15 cyber-attacks per day, amounting to a total of over 3 000 attacks – often in support of conventional military activity[2].

DECIPHERING CIOs

The widespread use of digital technologies has transformed the ways in which to wage the battle for 'hearts and minds'. Long-standing grievances have spilt over onto the amorphous borders of cyberspace. The two consecutive crises of the global pandemic and the Russian war of aggression against Ukraine have showcased the significance of influence operations. However, they have also highlighted the compounding impact of influence operations and cyber capabilities.

The significance of the so-called 'human domain' as a key arena of modern conflict has gained increasing traction[3]. Basically, this builds on the recognition that conflict is intrinsically tied to one key resource: the social, cultural, and psychological texture of individuals and groups. Efforts to win the support of a population as a tactic of war are of course nothing new: decades of counterinsurgency operations have shown that the population inhabiting a conflict zone is a key resource in determining the outcome of a campaign. The key innovation inherent to contemporary influence operations is that their resort to cyber means has expanded the conflicts' boundaries to a virtually unlimited space.

As this suggests, CIOs are influence operations that involve some degree of interaction with the layer of cyberspace as an enabler[4]. The hybrid nature of these operations derives from the fact that they rely on the actual use of force against a cyber infrastructure to produce an effect on the human domain – that is, to shape the attitudes, behaviour, or decisions of a target audience.

CIOs can thus be defined as operations with a cross-domain effect: by compromising a virtual infrastructure – courtesy of the cyber domain – they pave the way to achieving an impact in the broader human domain, where influence and perception are the main factors at play. There has been a proliferation of CIOs, leading to constant, high-volume, high-scale activities in cyberspace.

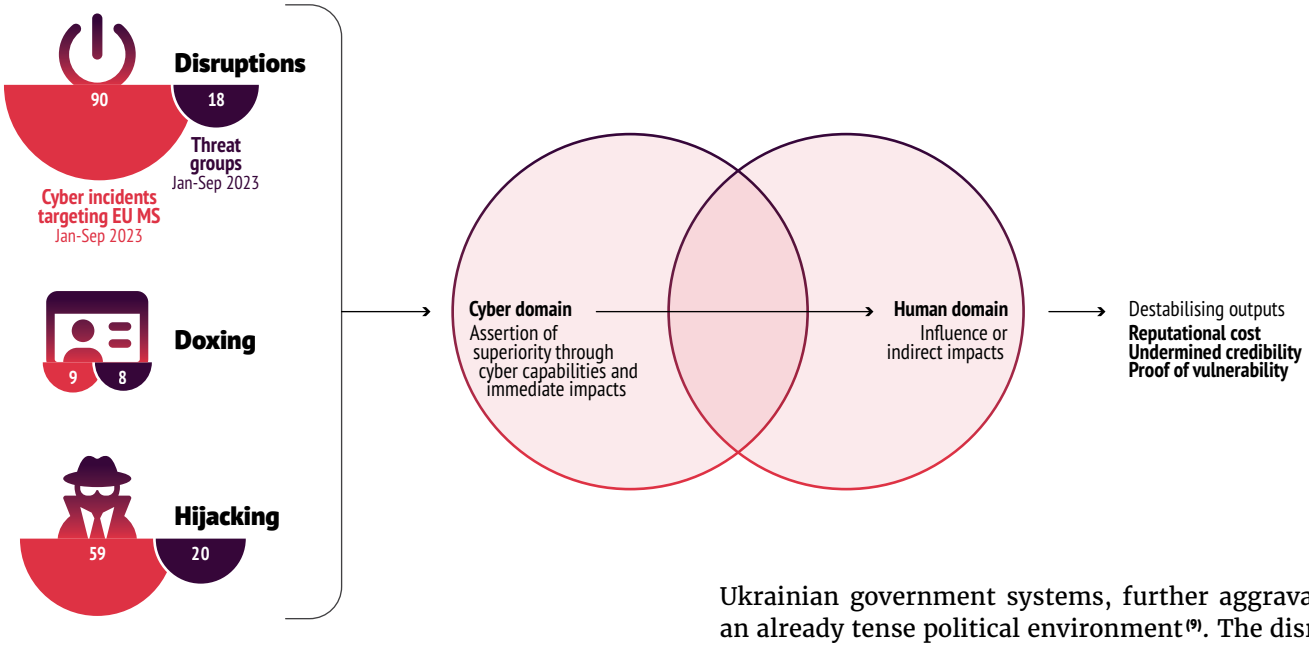
THE DRAW OF CIOs

CIOs can be compared to 'dirty bombs'. Their 'detonation' is the immediate impact of the cyberattack. In this analogy, the initial blast is followed by the dispersal of intangible components that explicitly seek to influence people's perceptions. A CIO's detonation thus occurs in the cyber domain, while its dispersal is directed at the human one.

The cyberattack has a powerful signalling value regardless of the magnitude of the actual harm it does. This signalling value is immediate: given that the primary objective of operations in the human domain is to destabilise and confuse adversaries, targeting and penetrating their digital infrastructure and systems can be very effective. While there are different means to achieve such a goal, they all entail an assertion of superiority and intend to erode the status of an opponent[5].

The effect of CIOs on the cyber and human domains

Conceptual diagram of intersection between cyber and human domain through CIOs



Data: EUREPOC, 2023

Furthermore, CIOs constitute ideal offensive capabilities. First because the barrier of access is low: 'cyber-crime as a service'[6] and 'cyber-mercenaries' have made malware, botnets and malicious tools[7] both affordable and readily available. Second CIOs are designed to be disruptive rather than destructive. Accordingly, they usually remain below the threshold of armed conflict and seldom result in direct retaliation[8]. This makes these operations intrinsically non-escalatory. Third, the veil of anonymity of cyberspace and the difficulty of attribution makes CIOs ideal for covert offensive activities. Finally, CIOs' return on investment has a multiplier effect. That is, while the impact of a single CIO might be negligible, a concatenation of multiple CIOs can produce a broader influence effect that – in turn – can benefit the broader strategic objectives of the perpetrating entities.

Before Russia's full-scale invasion of Ukraine in February 2022, expectations were high that cyberattacks would play a key role in Moscow's war effort, as they had in the invasion of Georgia. Instead, Russia's approach has been multifaceted, involving activities targeting the human domain to complement and support their broader strategic goals.

CIOs usually remain below the threshold of armed conflict and seldom result in direct retaliation.

Russia's defacement of Ukrainian government websites in January 2022 affords a good example of this approach. Although the attack drew on malware that deliberately complicated attribution, the incident sparked fear among Ukrainian officials that Russia had initiated a broader cyber campaign against Ukrainian government systems, further aggravating an already tense political environment[9]. The disruption of the Viasat Satellite network was another clear example of Russia's use of CIOs. The hack, which was strategically timed one hour before Russian troops crossed the border, aimed to degrade Ukrainian communication systems. The attacks simultaneously resulted in a spill-over that disrupted connectivity in several European countries[10].

Similarly, hackers linked to the Kremlin have engaged in a concerted campaign of doxing Ukrainian soldiers through channels like 'Work, brothers' and 'Tribunal', which have disclosed the private data of nearly 300 Ukrainian activists, soldiers and their families to over 120 000 subscribers[11]. Apart from the direct risks to the individuals involved, such operations underline Russia's effort to assert dominance in the information space.

Russia's cyber capabilities have not only targeted Ukraine, but over 20 other countries[12] that aligned with Kyiv. For instance, Moscow has used DDoS attacks through a hacker group called NoName057(16). Despite lacking technical sophistication, the group has disrupted various international entities, including Denmark's financial sector, Dutch ports, and Czech presidential candidate websites. NoName057(16) has been fully loyal to the Russian government. This was made clear through its decision to halt all other activity to target the Wagner mercenaries' sites during the failed mutiny on 24 June[13]. Another example of how NoName's activities fit into a broader human domain strategy is the attack on the websites of several Italian government institutions in March 2023. The group claimed responsibility for the incidents, framing the attack as

a retaliation against Italy's training of the Ukrainian military on anti-missile systems[14] .

Contrary to the widely anticipated 'Cyber Pearl Harbour', what has emerged is a pattern of disruptive cyber tactics used to support the kinetic war effort by influencing the information space around the war, while signalling Russia's cyber prowess.

THE WAY AHEAD

This Brief shows how CIOs target the intersection between the human and the cyber domains. They are part of multifaceted operations that aim to target strategic adversaries. Their impact on society and the global balance of power demonstrates the need to consider and develop countermeasures to manage the risks stemming from foreign interference operations. Current EU capabilities are tilted towards reacting to cyber assaults. This highlights the need for comprehensive strategies that recognise and address the intricate landscape of influence and perception in the cyber domain.

- **The centrality of coordination:** The dispersion of response capacities, even within a closely integrated system like the EU, impedes efforts to mount an effective response to the complex threats posed by cyber influence operations. A high degree of both vertical and horizontal coordination between Member States and EU institutions is essential to combat their multifaceted nature. Apart from regular institutional dialogue between specialised organisations, CIOs thus require coordination between cyber, intelligence and foreign policy agencies.
- **Recalibrating responses:** The EU has so far made relatively limited use of direct response tools. There seems to be a preference for using positive tools (such as capacity-building) that are directed at allies over negative tools (such as sanctions) directed at adversaries. While the posture-related value of the Cyber Diplomacy Toolbox still stands, the EU should consider recalibrating its actions towards adversaries in cases of prolonged and cumulative cyber operations.
- **Building technical and societal resilience to deter by denial:** Given the cross-domain effects of CIOs, resilience should be sought in both the human and cyber domains. Cyber threats often exploit relatively simple vulnerabilities, such as unpatched software, inadequate user credentials, or simple misconfigurations, therefore building technical resilience remains key. Similarly, strengthening the resilience of society *vis-à-vis* information campaigns helps to curb the ability to target perception and taint the information space.

References

(1) Taylor, J. and Basford Canales, S., 'Australia's home affairs department hit by DDoS attack claimed by pro-Russia hackers', *The Guardian*, 6 October 2023 (https://www.theguardian.com/australia-news/2023/oct/06/australia-department-of-home-affairs-ddos-hack-russia).

(2) Seldon, J., 'Ukraine, US intelligence suggest Russia cyber efforts evolving, growing', *VOA*, 7 September 2023. (https://www.voanews.com/a/ukraine-us-intelligence-suggest-russia-cyber-efforts-evolving-growing-/7259396.html).

(3) Branch, A., Cardon, E., Ellis, D. and Russell, A., 'We ignore the human domain at our own peril', Modern War Institute at West Point, 14 June 2021 (https://mwi.westpoint.edu/we-ignore-the-human-domain-at-our-own-peril/).

(4) We define a cyberattack as the 'use of computational technology in cyberspace for disruptive or destructive purposes'. See: European Repository of Cyber Incidents (EuRepoC) (https://eurepoc.eu/).

(5) Smith, D. J., 'How Russia harnesses cyberwarfare', *Defense Dossier*, Issue 4, 2012, pp. 7–8.

(6) Musotto, R., and Wall, D. S., 'More Amazon than Mafia: Analysing a DDoS stresser service as organised cybercrime', *Trends in Organized Crime*, Vol.25 No 2, 2020, pp. 1–19; Huang, K., Siegel, M., and Madnick, S., 'Systematically understanding the cyber-attack business: A survey', *ACM Computing Surveys (CSUR)*, Vol. 51, No 4, 2018, pp. 1–36.

(7) Maurer, T., *Cyber Mercenaries*, Cambridge University Press, Cambridge, 2018.

(8) Schmitt, M. N., '"Below the threshold" cyber operations: The countermeasures response option and international law', *Virginia Journal of International Law*, Vol. 54, 2013; Brangetto, P. and Veenendaal, M. A., 'Influence Cyber Operations: The use of cyberattacks in support of influence operations', 8th International Conference on Cyber Conflict, NATO CCD COE publication, Tallinn, 2016 (https://ccdcoe.org/uploads/2018/10/Art-08-Influence-Cyber-Operations-The-Use-of-Cyberattacks-in-Support-of-Influence-Operations.pdf).

(9) Council on Foreign Relations, 'Report: Targeting of Ukrainian government websites', January 2022 (https://www.cfr.org/cyber-operations/targeting-ukrainian-government-websites).

(10) Bateman, J., 'Russia's wartime cyber operations in Ukraine: Military impacts, influences, and implications', Carnegie Endowment for International Peace, 16 December 2022.

(11) 'We know where your family live' – Ukrainian fighters face online death threats', BBC News, 5 November 2022 (https://www.bbc.com/news/world-63491977).

(12) Hurel, L. M., 'On the promises and consequences of the intelligence contest in cyberspace', Royal United Service Institute, 23 August 2023 (https://www.rusi.org/explore-our-research/publications/commentary/promises-and-consequences-intelligence-contest-cyberspace).

(13) Kirichenko, D., 'Crowdsourced cyber warfare: Russia and Ukraine launch fresh DDoS offensives', 13 July 2023 (https://cepa.org/article/russia-ukraine-launch-cyber-offensives/).

(14) Redazione ANSA, 'Fresh wave of Russian cyberattacks on Italian sites', 22 March 2023 (https://www.ansa.it/english/news/general_news/2023/03/22/fresh-wave-of-russian-cyberattacks-on-italian-sites_62a61801-0ead-4b07-acb1-0648f8070c6c.html)

euiss

Published by the European Union Institute for Security Studies.
Printed in Luxembourg by the Publications Office of the European Union.

Cover image credit: Su San Lee/Unsplash

Publications Office of the European Union

PRINT ISBN 978-92-9462-201-3
CATALOGUE NUMBER QN-AK-23-019-EN-C
ISSN 2599-8943
DOI 10.2815/46683

PDF ISBN 978-92-9462-200-6
CATALOGUE NUMBER QN-AK-23-019-EN-N
ISSN 2315-1110
DOI 10.2815/429840