Cognitive Security: Facing Cognitive Operations in Hybrid Warfare[1]

Didier Danet
Saint-Cyr Military Academy, Guer, France

didier.danet@st-cyr.terre-net.defense.gouv.fr

Abstract: The digital space is now an active area of conflict. Attacks take many forms, to the point where concepts multiply and overlap. One concept in particular raises important questions: cognitive warfare. Cognitive warfare is an issue of concern to all countries, but there are very significant differences in approach between countries such as the United States or France and countries such as Russia, Iran or China. We try to show that these very different approaches leave Western countries unprepared for a global threat and poorly identified vulnerabilities. The concept of cognitive security therefore appears to be a promising avenue for reflection.

Keywords: Cyberdefense, Disinformation, Cognitive Warfare, Decision-Making Systems, Cognitive Security

1. Introduction

The digital space is an area of confrontation and conflict: cyber attacks, disinformation campaigns, espionage... In a world that is now “phygital”, distinguishing between the kinetic and non-kinetic dimensions of confrontations becomes more and more difficult, generating a certain confusion in concepts and categories. Hybrid war, electronic warfare, cyberwar, information warfare or cognitive warfare tend to overlap. This presentation is devoted to the concept of cognitive security, the interest of which is to take an overview of the operations carried out by certain countries such as Russia in intangible fields, to assess the threats and vulnerabilities and to propose appropriate responses.

2. From Information Operations to Cognitive Security: Old and New Threats

Cognitive warfare appears to be a concept still under construction in the various military doctrines of Western countries and their competitors. Amidst the diversity of interpretations that are given, a major difference between two main approaches is to be noted. Western countries emphasize the techno-scientific dimension and willingly link the notion of cognitive warfare to progress in bio-technologies and neuro-sciences. Countries like Russia have a more traditional approach. There, cognitive warfare is part of informational warfare.

2.1 The Western Approach to Cognitive Warfare: Technology First

In the West, many doctrinal documents pay attention to cognitive warfare. A common feature of this thinking is the tendency to favour a techno-scientific approach and to focus on the “weaponisation of biotechnologies and neuroscience”. (Giordano, 2017; Rickli and Ienca, 2021)

Thus, the French Minister of Defence mentioned “a new form of threat combining capabilities in information manipulation, disinformation, cybernetics, psychology, social engineering, biotechnology, and which could be summarised as a kind of new form of warfare: cognitive warfare. Cognitive warfare is the ability to exploit the vulnerabilities of the human brain using all the methods I have just mentioned.”

'This position is not isolated. Hacking the human brain is also a central element in the typology proposed by Hung and Hung. For these two authors, cognitive warfare and other types of warfare (information warfare, cyberwar…) “might contain the element of operations to influence and impact human cognition; however, only cognitive warfare is specifically dedicated to the control of the brain by incorporating militarised neuroscience into various practices”.(Hung and Hung, 2022)

2.2 The Russian Approach to Cognitive Warfare: Disinformation First

Originally, the major issues of cyber defense have revolved around attacks aimed at destroying or damaging vital military and industrial systems: administration, energy, transport, banks ... The attacks against Estonia (2007) or Georgia (2008) have attracted a lot of attention, and rightly so, since these attacks are still on the agenda with the invasion of Crimea (2015) and the Donbass (2022). The notion of "Cyber Pearl Harbor" reflects the fear of a

[1] The author thanks anonymous reviewers for providing helpful comments on earlier draft of the manuscript.

massive attack that could seriously disrupt or paralyze the entire life of a country or a region.(Dunn Cavelty, 2013; Lawson and Middleton, 2019)

But cyber-attacks such as the one against the French television channel TV5 Monde have shown that Russia can pursue another objective: to damage or destroy the image, reputation or credibility of its adversaries. (Brangetto and Veenendaal, 2016)

The "Doctrine of Information Security" formulates the ambition to guarantee Russia's sovereignty in cyberspace by providing "reliable information" on the policies of the country and its main leaders and by exercising digital influence. (Darczewska, 2015; Nocetti, 2015) This influence strategy mobilises all the media available in the digital space and ensures the unity and consistency of their discourse.

Historically, Russia's disinformation operations were first deployed in Europe.(Limonier and Audinet, 2017) Then, for a variety of reasons, they expanded to Southeast Asia and Africa.(Limonier, 2018)

In Europe, Russian disinformation operations involve the traditional media, particularly television channels, which have benefited from a sharp increase in budgets and resources since the beginning of the 2010s. (Fletcher *et al.*, 2018) Before the invasion of Ukraine and the sanctions imposed on RT and Sputnik, half of its viewers were in ten European countries including France, Germany and the United Kingdom.. In addition to the influence of traditional media on the Internet, social media are also very much in demand. The two dimensions are totally linked, as RT and Sputnik are very present on all applications such as Facebook, Twitter, Youtube, Instagram...

Since the mid-2010s, the cost-effectiveness of Russian disinformation operations in Europe has decreased, in particular thanks to the efforts undertaken by the European Union and its member countries to denounce these operations. Since the invasion of Ukraine, the two main vectors of Russian influence, RT and Sputnik, have been shut down, forcing Russia to change its focus.

In this respect, the African continent is a new priority. Until the end of the 2010s, Africa occupied a marginal place in Russian foreign policy, which was reflected in the very limited presence of cultural and media relays on the continent. In a very short period of time, this presence has increased dramatically, in particular as a result of an adaptation to the local context: a backbone based on two media (RT and Sputnik) and alternative and conspiracy-oriented content.

The adaptation to the local context is particularly impressive in terms of the construction of networks that promote the Russian vision.(Clifford and Gruzd, 2022) This adaptation also involves the diversification of the actors who carry Russian interests in the region. Alongside state media such as RT and Sputnik, private disinformation entrepreneurs are playing a very significant role. (Limonier and Laruelle, 2021) The result of this spectacular progression of Russian vectors of influence in Africa is a full-scale attack on the Western presence (especially the French) on the continent and, in particular, on the Barkhane military operation.(Douzet *et al.*, 2021)

In conclusion, it appears that the real threat facing Westerners in the field of cognitive warfare is not related to research programs aimed at 'hacking the brains' of individuals through biotechnology and neuroscience processes. Russia's actions in the digital space are part of a very classic policy of influence, but carried out with significant means, a global approach, a constant strategy and adaptation to the local context. (Strategic Communications, Task Forces and *et al.*, 2023) The real threat is therefore the ability of Russian propaganda to directly or indirectly influence Western decision-making processes and to challenge the image, reputation or credibility of the latter. This is where the issue of cognitive security comes in, given the vulnerabilities within Western decision-making systems.

3. Cognitive Threats: A Model

Russia's disinformation campaigns have raised awareness of the danger represented by influence operations aimed at destabilising institutions (TV5 Monde) or democratic processes (French presidential elections in 2017). The European Union and its member countries have reacted in several ways: ad hoc legislation or the creation of bodies to combat fake news such as the EU Disinformation Lab With the closure of RT and Sputnik following the invasion of Ukraine, it can be said that the threat has significantly diminished on the old continent. But we have seen that it has in fact moved to areas where our interests are now under pressure from influence campaigns, notably in Africa where France's positions are in difficulty with the imposed withdrawal of its armed forces from the Central African Republic, Mali and Burkina Faso. Above all, a new threat is emerging with the development of campaigns aimed at destabilising Western decision-making systems.

To highlight the nature and modalities of these "cognitive" campaigns, a simplified model of a collective decision-making process is proposed. It is an Agent / Environment / Decision model. The agent is a civil or military organisation which has a collective decision system integrating an expert/decision maker pair. This agent is given objectives. It observes the environment and takes decisions likely to lead to the objective. The decision process is of the OODA type.

To highlight the nature and modalities of these "cognitive" campaigns, a simplified model of a collective decision-making process is proposed. It is an Agent / Environment / Decision model. The agent is a civil or military organisation which has a collective decision system integrating an expert/decision maker pair. This agent is given objectives. It observes the environment and takes decisions likely to lead to the objective. The decision process is of the OODA type.

In the light of this model, three types of cognitive threats can be identified.

The first possible action concerns the environment in which the organisation must act and make decisions. As Dave Snowden has shown, a decision process of the type Sense / Analyse / Decide / Act (i.e. the OODA loop mechanism) is well suited to so-called complicated environments but where the universe remains ordered. (Snowden and Boone, 2007)

However, OODA-type decision-making processes can be destabilised in disordered environments, which Dave Snowden calls complex (cause and effect relationships seem to have disappeared even if patterns gradually emerge) or chaotic (no order can be discerned in an environment in crisis). The role of management teams changes profoundly and the appropriate leadership style is based on specific qualities such as the ability to take responsibility, to think outside the box and to bring solutions to the surface rather than to arbitrate. It is inferred that a possible attack on the decision-making systems of Western organisations, which are mainly based on OODA-type schemes, is to cause confusion or chaos in the environment. This can be interpreted as Russian propaganda in Africa manipulating public opinion in Mali or Burkina Faso, provoking demonstrations to block military convoys and placing those in charge of the convoys in situations that could degenerate very quickly.

The second type of cognitive attack is aimed at disrupting the critical cognitive infrastructure that allows deployed forces to receive the information they need, communicate with each other and maintain a constant link with headquarters. These attacks can be brutal, for example, the destruction of a communication system. They can be more insidious: flooding a communication channel to dilute relevant data in a sea of noise or altering the data flowing through the infrastructure.

This last type of attack directly targets the decision-making systems of Western organisations. The aim is to take advantage of existing vulnerabilities in these systems to make them commit significant errors that will prevent them from carrying out their missions or discredit them in the eyes of the population.

The next section will be devoted to an analysis of the possible vulnerabilities of Western decision-making systems.

4. Westen Organisations at Risk: Vulnerabilities

Faced with the three types of attack that the Agent/Environment/Decision model highlights, why might Western civilian or military organisations find themselves in trouble? The answer is well known to social scientists who are interested in the structures and processes of decision-making in organisations (management sciences, organisational sociology, behavioural psychology). There are three main reasons why collective decision-making systems go wrong. (Morel, 2002).

4.1 Cognitive Errors

The first source of error can be described as a "cognitive" error. The organisation does not have the necessary input data at the time it makes its decision. It does not have the right theories, concepts or tools to correctly understand the situation and the possible solutions. It engages in "cognitive tinkering" characterised by shortcuts in thinking, approximations in orders of magnitude, erroneous representations, etc. We have seen in relation to attacks on critical cognitive infrastructure that this can tend to introduce falsified data into decision-making systems. The latter then applies the analysis schemes and decision mechanisms correctly but, working from a representation of the environment that does not conform to reality, the decisions adopted are not adapted to the situation. Resources are wasted, the results obtained are not in line with the objectives, the organisation's action is mocked and its credit in the public opinion is degraded.

This type of cognitive attack is the most frequent and oldest mode. It is the one that the Russian eco-system has been engaging in in Africa since the mid-2010s.

The second type of cognitive error does not involve any particular manoeuvre by the adversary. It is more simply a "defeat of thought". The organisation that is given a mission does not make the effort to understand the terrain, is satisfied with simplifying reading grids, a supposed knowledge based on experience and, in short, a damaging intellectual laziness.

Finally, the representation error consists of transposing a certain conception from a source domain where it may be relevant to a target domain where there is no guarantee that it will be relevant. This type of error is related to what Daniel Kahneman calls “cognitive tinkering”. (Kahneman, 2012) One could quickly summarise this point by saying that “cognitive tinkering” consists of an organisation substituting a mode of reasoning based on intuition for a mode of reasoning of an analytical nature. This bricolage can be explained by many reasons: the sense of urgency, the impression of having already encountered a comparable situation, the weight of prejudices, the strength of intuition...

4.2 Collective Errors

Collective errors are inherent in the structure and functioning of groups (experts / decision-makers) that have to make a decision. It is widely recognised that a group decision mobilises different skills and abilities, which enriches the thinking and decision-making process, generally producing more relevant decisions. However, it should not be ignored that the group does not always function well and that dysfunctions may appear which will be the cause of collective errors.

A first source of collective error comes from a poor structuring of the group and the distribution of roles within it. For example, excessive fragmentation of decision-making groups creates "gaps" which are sources of friction and poor information transmission The adversary has little ability to influence the structure of such groups. But the bureaucratic nature of Western organisations, especially when they are public or international, tends to generate this type of vulnerability.

The second type of collective error is related to the poor functioning of groups. This functioning can be affected by multiple difficulties. The group may be excessively inward-looking and lose contact with its environment. This risk exists, for example, when a Western organisation is projected into a theatre of crisis or war and locks itself up in fortified camps for understandable security reasons. However, this confinement can produce a form of watertightness that is damaging to local actors and the Western actors. Another example is the communication procedures within a decision-making group. We are thinking here of the phenomena of "groupthink" (Janis, 2008) or the excess of implicit communication or the refusal of procedures aimed at formalising exchanges within the group...

This is not to say that Western organisations are riddled with weaknesses in their structures and collective functioning. One could even argue that, given the performance of the Russian army in Ukraine, our adversaries are probably even more affected than we are. But there is no reason to believe that Western organisations are immune and not at risk of making collective mistakes. The problem is that they are not diagnosed and the risk can arise here and there without being anticipated.

4.3 The Collapse of Sense-Making

Finally, the most serious mistakes come from the collapse of sense-making. As Karl Weick has shown, the collapse of meaning means that a group loses sight of the goal and focuses on the means. (Weick, 1993) The priority that should be given to the "why" of the action disappears in favour of the "how" of acting in uncertainty. This can have dramatic consequences as the objective is lost sight of and the implementation of the group's technical skills can lead in a completely different direction from that desired.

In difficult environments, trust and cohesion are two crucial characteristics of teams that do not collapse. Trust and cohesion may be jeopardized because of targeted influence campaigns. These operations make extensive use of the presence of civilian or military personnel in digital space (“digital fingerprinting”). The issue of “digital fingerprinting” was first raised because of the information leaks that can result from carelessness on the part of personnel on mission. The case of Strava watches used by military personnel to record their sporting activities has been widely studied and commented upon. (Cattaruzza and Taillat, 2018; Mericskay, Noucher and Roche, 2018; Condorcet, 2020) Similarly, the impact of videos or messages posted on social networks is the subject of increasingly common best practice guides. These mistakes obviously have consequences, not least because of

the spectacular development of OSINT techniques and tools. (Limonier 1 and Audinet 2, 2022; Renault 1, Charon 2 and Laurençon 3, 2022)

In addition to the problem of data leakage, the presence of people in the digital space opens the way for targeted influence operations that aim to undermine the trust of individuals in institutions, in their leaders or in their peers. This is not to say that all social networks inevitably breed distrust and division. But some of them base their ability to attract and retain users on such processes. For example, Facebook was a privileged vector of Russian influence during the US (2016) or French (2017) presidential elections insofar as the application exacerbates social feedback loops and emotional reactions.(Figeac *et al.*, 2019)

In conclusion, it appears that Western organisations deployed in crisis or conflict areas are weakened by the vulnerability of their collective decision-making processes. These vulnerabilities are characteristics common to all organisations. However, not all organisations have the same sources of vulnerability or the same degree of fragility due to these vulnerabilities. The problem is not to stigmatise the existence of these sources of vulnerability and the ambition should not be to eliminate them entirely. On the other hand, it is quite dangerous not to have a comprehensively designed and periodically applied assessment system. Ignorance of the current state of organisations, particularly those operating in difficult environments where the risks of Russian influence operations are known, does not allow for the anticipation of problems that may arise and does not allow for measures to be taken to strengthen “prone-crisis” organisations.

5. Enhancing Cognitive Security in Crisis Environments

Identifying threats related to Russian influence operations in both Europe and Africa, combined with the likely vulnerabilities of Western decision-making systems, leads to suggest measures to ensure the cognitive security of these systems. These recommendations can be classified according to the three types of attacks that have been underlined.

5.1 Cognitive safety in the face of environmental degradation

In disordered universes (complex or chaotic), the OODA loop (or Sense / Analyse / Decide / Act) is no more relevant and decision-makers must turn to processes where they must think outside the box, take the risk of acting without certainty and assume significant responsibilities in the event of failure. Three sets of measures are suggested to strengthen the cognitive security of the organisation.

First, anticipating adverse moves. Russian informational attacks follow relatively simple and constant patterns. (Chew and Turnley, 2017; Innes and Dawson, 2022; Olchowski, 2022) The propaganda arguments are few and relatively crude: the colonial past of the West, the hidden economic underpinnings of their interventions, the alternative reality and the conspiracies... (Nocetti, 2015) Similarly, the vectors of these operations are well identified: official Russian media and local partners, social networks of oligarchs and associated African entrepreneurs... It is therefore possible to anticipate informational attacks or to detect them at the earliest stages of their development.

Second, countering Russian narratives involves both refuting and responding to them. The actions to be taken are not always simple. In 2020, Facebook announced that it had closed 150 fake accounts, some linked to Russia and others to the French army. According to a Graphika report, the fake accounts linked to the French army were intended to respond to a Russian campaign in Mali by countering accusations of neo-colonialism with "posts" and cartoons focusing on the looting of mining resources by the mercenaries of the Wagner Group. (Graphika & the Stanford Internet Observatory, 2020) However, the ‘faux-nez’ used to carry out this retaliation were not sufficiently refined to escape Facebook's control procedures. Conversely, Western actions can be successful. For example, in April 2022, French forces in the Gossi region of Mali were able to film mercenaries from the Wagner Group staging a fake mass grave in order to accuse the French army. The dissemination of the images provided evidence of a staged operation aimed at turning the population against Operation Barkhane. (Robin, 2022)

Finally, if attacks result in significant environmental degradation, decision-makers must be prepared to engage in complexity or chaos management procedures. It is then necessary to ensure that all actors on the ground have these particular capabilities and, if these are not deemed complete enough, to set up training and education programs.

5.2 Cognitive security in the face of attacks on critical cognitive infrastructure

Attacks on critical cognitive infrastructure can be easily detected, especially when they aim to interrupt the attacked organisation's ability to perceive the environment and communicate. The destruction of a submarine cable or a terrestrial network is immediately perceived by users. However, if the attacker's aim is to drown the target in a flood of false information or noise, the intervention is more difficult to perceive. Therefore, three measures could be useful in this case.

The first is to systematically establish territorial connectivity diagnostics. These diagnoses aim to assess the digital information flow capacities in a given region, in particular the capacity that an operator such as Russia might have to divert internet flows to traffic nodes where it would be able to control and modify their content.

A second set of measures could aim at strengthening data-centric security measures. (Bayuk, 2009; Hennessy *et al.*, 2009; Arora, Raja and Bahl, 2018) These technical measures consist of ensuring that sensitive data is stored and circulates under the control of the organisation. For example, specific devices check that such data is not sent to unauthorised recipients or that it is present in certain areas of the information system. Such measures already exist in many organisations. They should be evaluated and strengthened if necessary.

Finally, the information systems security paradigm could be questioned as it seems to have reached certain limits. Traditionally, the protection of information systems has been seen as a fortress whose walls must be constantly raised to cope with the growing resources of attackers. However, the requirements of security designed in this way are becoming increasingly onerous and breaches due to the "human factor" are multiplying. Some authors advocate the development of a new approach in which the fortress is considered to be already invaded, thus forcing new behaviours on the part of the defenders of the system and its users. (Leuprecht, Skillicorn and Tait, 2016)

5.3 Cognitive security and the Collapse of Sense Making

Not all organisations are equal when faced with difficult, crisis or conflict situations. Some collapse ("prone-crisis organisations") (Mitroff *et al.*, 1989; Pauchant and Mitroff, 1992) while others prove surprisingly resilient (Highly Reliable Organisations). The parameters that explain this difference in response have been well identified in the academic literature. (Roberts, 1990) It is all the more surprising to note that audit mechanisms are not systematically put in place to identify and correct any weaknesses. The risks linked, for example, to an oversimplification of the grids for understanding situations or to an excessive polarisation of opinions within a unit should, in our opinion, be the subject of particular attention.

6. Conclusion

The term "cognitive warfare" has generated a certain amount of excitement, fuelled in particular by the spectacular progress of various scientific disciplines such as biotechnology, neuroscience and artificial intelligence. However, defining cognitive warfare by the famous expression "hacking the enemy's brain" amounts to focusing on a hypothetical threat, whereas our adversaries are practising a less sophisticated but equally dangerous "cognitive warfare", in particular because of the ignored vulnerabilities in our information and decision-making systems. Cognitive warfare should mainly be seen as an extension of information warfare. In this respect, threat analysis has made great progress, as demonstrated by the documents recently published by the European Union. (ENISA and EEAS, 2022; Strategic Communications, Task Forces and *et al.*, 2023) In particular, knowledge of the Russian disinformation eco-system, the analysis of the behaviour of actors or the study of speeches allows for early detection and a more appropriate response to disinformation manoeuvres. However, a grey area remains in this picture: the analysis of vulnerabilities that are exploited by attackers to achieve their objective. It is these organisational vulnerabilities that need to be better explored to address the threat of cognitive warfare.

References

Arora, A.S., Raja, L. and Bahl, B. (2018) 'Data centric security approach: A way to achieve security & privacy in cloud computing', in *Proceedings of 3rd International Conference on Internet of Things and Connected Technologies (ICIoTCT)*, pp. 26–27.

Bayuk, J. (2009) 'Data-centric security', *Computer Fraud & Security*, 2009(3), pp. 7–11.

Brangetto, P. and Veenendaal, M.A. (2016) 'Influence cyber operations: The use of cyberattacks in support of influence operations', in *2016 8th International Conference on Cyber Conflict (CyCon)*. IEEE, pp. 113–126.

Cattaruzza, A. and Taillat, S. (2018) 'Les enjeux de la numérisation du champ de bataille', *Dynamiques internationales* [Preprint], (13).

Chew, P.A. and Turnley, J.G. (2017) 'Understanding Russian information operations using unsupervised multilingual topic modeling', in *Social, Cultural, and Behavioral Modeling: 10th International Conference, SBP-BRiMS 2017, Washington, DC, USA, July 5-8, 2017, Proceedings 10*. Springer, pp. 102–107.

Clifford, C. and Gruzd, S. (2022) 'Russian and African media: Exercising soft power', *South African Institute of International Affairs Policy Insights,(125)*, 1, p. 18.

Condorcet, A.C. (2020) 'Quelle place pour les cartes dans l'analyse politique de l'espace?'

Darczewska, J. (2015) *The devil is in the details. Information warfare in the light of Russia's military doctrine*. Warsaw: OSW Center for Eastern Studies (Point of View, 50).

Douzet, F. *et al.* (2021) 'Mapping the spread of Russian and Chinese contents on the French-speaking African web', *Journal of Cyber Policy*, 6(1), pp. 50–67.

Dunn Cavelty, M. (2013) 'Un Cyber Pearl Harbor : quelle probabilité à court terme ?', *Défense Sécurité Internationale (DSI)*, Numéro Spécial(32), pp. 30–32.

ENISA and EEAS (2022) *Foreign Information Manipulation Interference (FIMI) and Cybersecurity - Threat Landscape*, *ENISA*. Available at: https://www.enisa.europa.eu/publications/foreign-information-manipulation-interference-fimi-and-cybersecurity-threat-landscape (Accessed: 23 February 2023).

Figeac, J. *et al.* (2019) 'Facebook favorise-t-il la désinformation et la polarisation idéologique des opinions?', *Questions de communication*, (36), pp. 167–187.

Fletcher, R. *et al.* (2018) 'Measuring the reach of" fake news" and online disinformation in Europe', *Australasian Policing*, 10(2).

Giordano, J. (2017) 'Weaponizing the brain: Neuroscience advancements spark debate', *National Defense*, 6, pp. 17–19.

Graphika & the Stanford Internet Observatory (2020) *More-Troll Kombat*. Available at: https://graphika.com/reports/more-troll-kombat/ (Accessed: 10 February 2022).

Hennessy, S.D. *et al.* (2009) 'Data-centric security: Integrating data privacy and data security', *IBM Journal of Research and Development*, 53(2), pp. 2–1.

Hung, T.-C. and Hung, T.-W. (2022) 'How China's Cognitive Warfare Works: A Frontline Perspective of Taiwan's Anti-Disinformation Wars', *Journal of Global Security Studies*, 7(4), p. ogac016.

Innes, M. and Dawson, A. (2022) 'Erving Goffman on misinformation and information control: the conduct of contemporary Russian information operations', *Symbolic Interaction*, 45(4), pp. 517–540.

Janis, I.L. (2008) 'Groupthink', *IEEE Engineering Management Review*, 36(1), p. 36.

Kahneman, D. (2012) *Thinking Fast and Slow*. Available at: https://www.youtube.com/watch?v=GrFHRtGmE5I.

Lawson, S. and Middleton, M.K. (2019) 'Cyber Pearl Harbor: Analogy, fear, and the framing of cyber security threats in the United States, 1991-2016', *First Monday*, 24(3).

Leuprecht, C., Skillicorn, D.B. and Tait, V.E. (2016) 'Beyond the Castle Model of cyber-risk and cyber-security', *Government Information Quarterly*, 33(2), pp. 250–257.

Limonier 1, K. and Audinet 2, M. (2022) 'De l'enquête au terrain numérique: les apports de l'Osint à l'étude des phénomènes géopolitiques', *Hérodote*, (3), pp. 5–17.

Limonier, K. (2018) 'Diffusion de l'information russe en Afrique: essai de cartographie générale', *Note de recherche*, 66.

Limonier, K. and Audinet, M. (2017) 'La stratégie d'influence informationnelle et numérique de la Russie en Europe', *Hérodote*, (1), pp. 123–144.

Limonier, K. and Laruelle, M. (2021) 'Russia's African Toolkit: Digital Influence and Entrepreneurs of Influence', *Orbis*, 65(3), pp. 403–419.

Mericskay, B., Noucher, M. and Roche, S. (2018) 'Usages des traces numériques en géographie: potentiels heuristiques et enjeux de recherche', *L'information géographique*, (2), pp. 39–61.

Mitroff, I.I. *et al.* (1989) 'Do (some) organizations cause their own crises? The cultural profiles of crisis-prone vs. crisis-prepared organizations', *Industrial Crisis Quarterly*, 3(4), pp. 269–283.

Morel, C. (2002) 'Les décisions absurdes', *Paris, Gallimard*, 2012.

Nocetti, J. (2015) 'Guerre de l'information: le web russe dans le conflit en Ukraine', *Focus Strat*, 62, pp. 1–47.

Olchowski, J. (2022) 'How to Weaponise Information: Russian Patterns', in *Disinformation, Narratives and Memory Politics in Russia and Belarus*. Agnieszka Legucka&Robert Kupiecki. Routledge, pp. 59–71.

Pauchant, T.C. and Mitroff, I.I. (1992) *Transforming the crisis-prone organization: Preventing individual, organizational, and environmental tragedies*. Jossey-Bass.

Renault 1, C., Charon 2, P. and Laurençon 3, F. (2022) 'Renseigner autrement? Trajectoires de l'Osint dans les services de renseignement', *Hérodote*, (3), pp. 19–30.

Rickli, J.-M. and Ienca, M. (2021) 'The security and military implications of neurotechnology and artificial intelligence', *Clinical Neurotechnology Meets Artificial Intelligence: Philosophical, Ethical, Legal and Social Implications*, pp. 197–214.

Roberts, K.H. (1990) 'Some characteristics of one type of high reliability organization', *Organization Science*, 1(2), pp. 160–176.

Robin, M. and Kimberly (2022) *La doctrine cyber française, continuité et renforcements depuis 2008. La politique cyber française durant le mandat d'Emmanuel Macron (2017-2022).* Louvain: UCL, Faculté des sciences économiques.

Snowden, D.J. and Boone, M.E. (2007) 'A leader's framework for decision making', *Harvard business review*, 85(11), p. 68.

Strategic Communications, Task Forces and *et al.* (2023) *1st EEAS Report on Foreign Information Manipulation and Interference Threats | EEAS Website*. Brussels: European External Action Service. Available at: https://www.eeas.europa.eu/eeas/1st-eeas-report-foreign-information-manipulation-and-interference-threats_en (Accessed: 11 February 2023).

Weick, K.E. (1993) 'The collapse of sensemaking in organizations: The Mann Gulch disaster.', *Administrative science quarterly*, 38(4), pp. 628–652.