Osinter et *red teamer*
Les corsaires du cyberespace

Philippe Lépinard
Univ Paris Est Créteil, IRG,
Krithika Yasonthiram
Univ Paris Est Créteil, IAE Paris-Est

Résumé :
L'objectif de notre article est d'entamer une discussion avec la communauté scientifique en management des systèmes d'information (MSI) autour des pratiques civiles émergentes de l'*Open Source Intelligence* (OSINT) et du *red teaming* en parallèle de leur montée en puissance au sein des forces armées françaises. En effet, et contrairement aux matériels militaires classiques, l'accessibilité des outils et dispositifs de formation nous invitent à nous questionner sur la future structuration du domaine cyber dans des contextes de tensions et de conflits interétatiques. Afin d'appréhender cette dynamique, nous proposons de l'aborder grâce au concept de *digital undertow* d'Orlikowski & Scott (2023) afin de mettre en avant les risques de morcellement de la communauté cyber entre pirates et corsaires au gré des évolutions géopolitiques mondiales.

Mots clés :
Renseignement Origine Sources Ouvertes ; Red team ; Cybersécurité ; Multimilieux multichamps

Osinter and red teamer
The corsairs of cyberspace

Abstract :
The aim of our paper is to initiate a discussion with the Information Systems Management (MSI) scientific community around the emerging civilian practices of Open Source Intelligence (OSINT) and red teaming, alongside with their rise to prominence within the French armed forces. Indeed, unlike conventional military equipment, the accessibility of training tools and systems prompts us to question the future structuring of the cyber domain in contexts of inter-state tension and conflict. To understand this dynamic, we propose to approach it using

Orlikowski & Scott's (2023) concept of digital undertow, in order to highlight the risks of fragmentation of the cyber community between pirates and privateers as global geopolitical developments unfold.

Keywords :
Open Source Intelligence ; Red team ; Cybersecurity ; Joint All Domain Operations

Osinter et *red teamer*
Les corsaires du cyberespace

« Des forces et des acteurs protéiformes y [l'espace opérationnel, NDA] *évoluent sur un spectre compétition – contestation – affrontement (CCA) qui rend caduque la notion de « temps de paix ».*
(Besse, 2023, p.62)

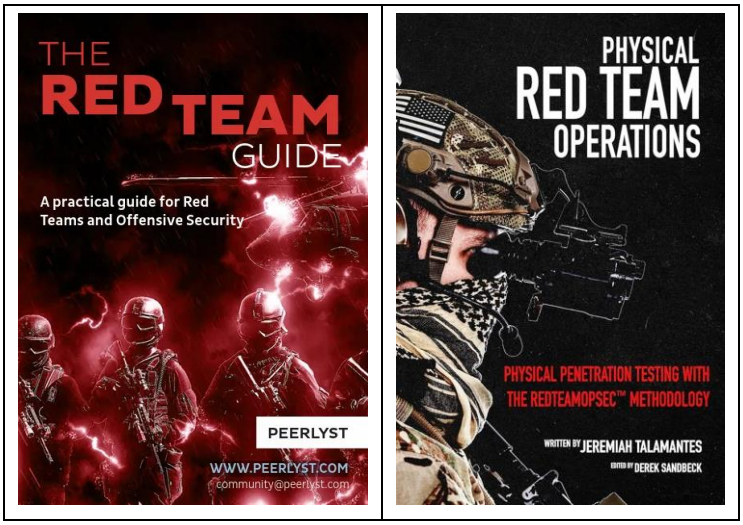
Introduction

En 2021, le chef d'état-major des armées françaises, le général d'armée Burkhard, présentait sa vision stratégique. Dans ce document initiant sa prise de fonction, il aborde notamment le triptyque compétition – contestation – affrontement afin de remplacer le continuum plus classique de paix – crise – guerre jugé dorénavant peu pertinent pour « *appréhender la conflictualité dans toute sa complexité* » (Burkhard, 2021, p.8). En parallèle, nous assistons à l'émergence du concept de multi-milieux multi-champs (M2MC) qui désigne « *le cadre d'engagement des opérations militaires contemporaines connectées, dans lesquelles les armées mettent en œuvre des modes d'actions au sein même de chaque milieu ou champ ou depuis les uns vers les autres* » (Gros *et al.*, 2021, p.18). Le M2MC couvre actuellement cinq milieux (terrestre, maritime, aérien, extra-atmosphérique et cyber[1]) et deux domaines (électromagnétique et informationnel). Cette approche doit toutefois être appréhendée à l'aune du concept d'intégration visant « *une synchronisation et une combinaison de toutes les décisions et actions susceptibles de produire une gamme d'effets élargis* » (Luzeaux, 2023, p.17). D'ailleurs, le général Burkhard (2021, p.9) précise que, dans le cadre de la compétition, « *l'objectif est de gagner la guerre avant la guerre, en agissant en tant que de besoin dans tout ou partie des champs et milieux* ». C'est précisément dans ce contexte que notre travail s'inscrit. En effet, s'il est possible d'appréhender militairement les milieux conflictuels terrestre, maritime, aérien et extra-atmosphérique compte tenu des moyens physiques déployés et de leurs effets visibles sur le théâtre des opérations (lui-même relativement circonscrit), ce n'est à notre avis pas le cas concernant le milieu cyber puisque les outils et techniques ne sont pas spécifiques aux militaires ; ce qui entraîne une dissipation, peut-être à terme incontrôlable, de la frontière entre les domaines militaire et civil (le champ lexical et figuratif est d'ailleurs largement commun, cf. Figures 1 et 2) : « *la cyberguerre entre la Russie et l'Ukraine abolit tous les repères connus. Qui se bat, sur quel terrain, sous quel drapeau et avec quelles limites ?* » (« Hacktivisme et guerre », 2023, p.31).

Dans le cadre de notre article, nous souhaitons aborder deux métiers caractérisés par leur forte ambivalence (notamment historique) civile et militaire : *osinter* et *red teamer*. L'objectif est donc d'entamer une discussion avec la communauté scientifique en management des systèmes d'information (MSI) autour des pratiques émergentes de l'OSINT et du *red teaming* au-delà des

[1] Selon le ministère des Armées (Agence Innovation Défense, 2022, p.18), les activités liées à la cyber couvrent deux grands domaines : la cybersécurité (protection et défense) et l'action numérique (influence et lutte informative offensive).

seuls aspects légaux qui peuvent être rapidement mis à mal dans des contextes de tensions, voire de conflits, interétatiques.



Figures 1 & 2. Premières de couverture de deux ouvrages sur le red teaming en cybersécurité (Frazer & Miller, 2020 ; Talamantes, 2019). La métaphore avec le domaine militaire est particulièrement explicite.

1. L'*Open Source Intelligence*

Le Renseignement d'Origine Source Ouverte (ROSO) ou, plus communément nommé, *Open Source Intelligence* (OSINT) est « *the methodical collection and exploitation of information from publicly available sources to fulfil an intelligence requirement* » (Block, 2023, p.3). Plus précisément, Abbas (2023, p.5) nous indique que l'OSINT « *refers to the gathering, processing, analyzing, producing, classifying, and disseminating data received from various sources and by techniques that are both open to the public and legally accessible and able to be used by the general public in response to official requests national security considerations* ». Il regroupe six grandes catégories de sources d'information : « *presse et média, Internet (publications, blogs, réseaux sociaux, contenus vidéos), données gouvernementales publiques, publications académiques et professionnelles spécialisées, données commerciales, littérature grise (rapports techniques, prépublications, newsletters, etc.)* » (Renault *et al*., 2022, p.20).

Si la pratique de l'OSINT est certainement aussi ancienne que l'humanité, sa structuration documentée est plutôt récente puisque les premiers textes formels dates de la fin du 20e siècle (cf. Block, 2023, pour un historique complet remontant au début du 17e siècle et avec un focus saisissant sur la guerre civile américaine). Steele (1990) serait peut-être l'un des premiers auteurs à nommer explicitement ce concept (p.31). La pratique de l'OSINT regroupe des outils largement accessibles au grand public grâce, entre autres, à l'OSINT Framework[2] et à différents sites de formation ou d'entraînement gratuits comme les plateformes OZINT[3] et *The OSINT Project* (TOP)[4]. La guerre russo-ukrainienne l'a mis largement sur le devant de la scène et de

[2] Site Internet de l'OSINT Framework : https://osintframework.com/.
[3] Site Internet de la plateforme OZINT : https://ozint.eu/.
[4] Site Internet de la plateforme TOP du Campus Cyber : https://the-osint-project.fr/.

nombreux influenceurs ou journalistes s'appuient sur ces sources ouvertes pour informer le public ou mener des actions de contre-enquête numérique (ou *fact-checking*)[5]. Le site Oryx est à ce titre devenu incontournable pour le recensement des pertes matérielles ukrainiennes et russes[6]. L'OSINT regroupe donc des pratiques totalement duales qui peuvent être menées par des militaires en opérations mais également des civils dans un contexte de tension (et bien entendu de conflit) interétatique. Le Deuff & Roumanos s'interrogent à ce propos (2021, p.25) : « *Son attractivité et son accessibilité* [OSINT, NDA] *obligent néanmoins à interroger les risques d'ordre sécuritaire, analytique et éthique qui le traversent, d'autant qu'il s'agit d'un champ très vaste et parfaitement ouvert à quiconque dispose d'un certain bagage informatique* ». Pour cette raison, plusieurs professionnels de l'OSINT ont proposé en 2023 un livre blanc destiné à réfléchir sur son cadre légal[7]. Mais quel peut être réellement sa portée dès lors que n'importe quel citoyen curieux disposant d'un accès à Internet et d'un peu d'appétence informatique peut s'engager proactivement dans un conflit interétatique (le concernant ou non) en recueillant et exploitant des sources ouvertes ?

2. *Red team*

Le *red teaming* est une activité dont la frontière avec le monde de la défense est encore plus effacée que pour l'OSINT. En effet, elle est issue de la formation militaire et, plus particulièrement de l'usage des *wargames* : « *En France, le red teaming est généralement envisagé comme une manière de se mettre à la place de l'ennemi, une pratique qui se décline au niveau stratégique, opératif et tactique* » (Fayet & Férey, 2023, p.4). Dans le cadre de la cybersécurité, le *red teaming* est « *a disciplined and systematic approach that adopts offensive strategies to bolster defensive capabilities* » (McLaughlin, 2023, p.18). Il est donc destiné à tester les défenses cyber des organisations dans un cadre contractuel (et donc légal). Nous nous situons donc ici dans une approche de *hacking* éthique parfaitement reconnu mais avec un périmètre d'actions et de méthodes plus larges que le test d'intrusion (*pentesting*) ; notamment parce que les équipes de cybersécurité de l'organisation testée ne sont pas au courant des attaques et parce que des dispositifs d'ingénierie sociale poussés et des tests d'intrusion physique sont mis en œuvre[8]. Les compétences d'une équipe *red team*, à la fois techniques mais également organisationnelles, sont telles qu'elles sont totalement et naturellement transposables à des attaques réelles. En effet, certains indices nous permettent de penser que des *hackers* éthiques de pays démocratiques prennent part directement ou indirectement dans l'un des conflits interétatiques actuels.

---

[5] Plusieurs situations cocasses peuvent émerger de l'OSINT. Par exemple, les deux journalistes français Xavier Tytelman (Air & Cosmos, pro-Ukraine) et Xavier Moreau (STRAPOL, pro-Russie) se livrent une bataille de chiffres par médias interposés en s'appuyant tous deux sur des sources ouvertes.

[6] Site Internet Oryx : https://www.oryxspioenkop.com/.

[7] Lien vers la page de téléchargement du « *Livre blanc le cadre légal de l'OSINT - Réflexion intercommunautaire* » : https://ozint.eu/livre-blanc-cadre-legal-2023/ (consulté le 14 janvier 2024.

[8] La vidéo « Les bases de la *red team* » diffusée sur la chaîne YouTube HacktBack est particulièrement intéressante pour comprendre l'approche « forces spéciales » du *red teaming*. L'un des invités est d'ailleurs un ancien militaire : https://urlz.fr/pgcF.

3. *Digital undertow*

Les *osinters* et *red teamers* sont-ils les futurs corsaires selon la distinction classique entre pirate et corsaire ; ces derniers se différenciant non pas par leurs actions (les mêmes que les pirates) mais par l'habilitation qu'ils possèdent provenant de leurs dirigeants ? Si cette distinction peut paraître superficielle, elle questionne pourtant le plus haut niveau de gouvernance de certains États. Par exemple, le Conseil fédéral suisse indique que « *la promotion du piratage éthique vise à offrir aux pirates les meilleures incitations possibles pour qu'ils utilisent leurs compétences dans l'esprit du piratage éthique et contribuent ainsi à la cybersécurité* [au niveau du pays, NDA] » (Conseil fédéral suisse, 2023, p.3). Cette démarche nous interpelle car elle peut finalement être éclairée par le concept de *digital undertow* proposé par Orlikowski & Scott (2023) qui indique, qu'au-delà des changements et conséquences visibles de la transformation numérique, des dynamiques émergentes supplémentaires beaucoup plus diffuses sont également à l'œuvre. Ces évolutions sous-tendent des tensions qui peuvent mener soit au renforcement institutionnel soit à son déplacement (menace existentielle pour l'organisation, *ibid.*, p.10). Par l'intégration formelle du cyber dans les milieux conflictuels, il nous semble possible d'avancer que l'État français a généré les tensions tactiques du *digital undertow*. La question est donc de savoir si les armées françaises vont être capables d'absorber les forces en mouvement de la cyber actuelle (via par exemple la structuration du *reach-back*[9]) ou si elles risquent un morcellement cyber incontrôlable mêlant des forces militaires et des forces civiles ou paramilitaires à l'image de communautés (comme Bellingcat[10]) ou de groupes de mercenaires pourtant interdit par la loi française du 14 avril 2003 relative à la répression de l'activité de mercenaire ?

Références

Abbas, S. S. (2022). History Of OSINT. In *Osint Investigations: We Know what you did that Summer* (pp. 8-11). Information Warfare Center.

Besse, J.-P. (2023). C2 Multi-milieux multi-champs (M2MC) : imposer la complexité sans la subir. *Revue Défense Nationale*, HS11, 53-69.

Block, L. (2023). The long history of OSINT. *Journal of Intelligence History*, à paraître.

Burkhard, T. (2021). *Vision stratégique du chef d'état-major des armées*. Ministère des armées.

Clark, B., & Downer, N. (2022). *Red Team Field Manual, Version 2*, Mike Mangrum.

Conseil fédéral suisse (2023). *La promotion du piratage éthique en Suisse*. Confédération suisse.

Fayet, H. & Férey, A. (2023). « Imaginer au-delà de l'imaginaire » Red teaming et serious games au service de l'anticipation et de la prospective. *Briefings de l'IFRI*, 1-14.

Frazer, D. & Miller, A. (2020). *The Red Team Guide. A practical guide for Red Teams and Offensive Security*, Peerlyst.

[9] *« Reach-back support is a relatively new concept. It provides operational warfighting units -battalions and brigades - the opportunity to reach outside of their traditional avenues of information flow and use national intelligence community assets to gather information to fill "gaps" in tactical intelligence* » (Radzikowski, 2008, p.24).

[10] Site Internet du groupe Bellingcat : https://fr.bellingcat.com/.

Gros, P., Tourret, V., Mazzucchi, N., Fouillet, T. & Wohrer, P. (2021). *Intégration multimilieux / multichamps : enjeux, opportunités et risques à horizon 2035*. Fondation pour la recherche stratégique.

Hacktivisme et guerre (2023). *Pirate informatique*, 30-31.

Loi n° 2003-340 du 14 avril 2003 relative à la répression de l'activité de mercenaire.

Luzeaux, D. (2023). Le numérique au service du combat collaboratif. *Revue Défense Nationale*, 865, 17-23.

McLaughlin, K. L. (2023). Offense for Defense: The Art and Science of Cybersecurity Red Teaming. *The EDP Audit, Control, and Security Newsletter*, *67*(5), 18-24.

Agence Innovation Défense (2022). *Document de référence de l'orientation de l'innovation de défense*. Ministère des Armées.

Orlikowski, W. & Scott, S. (2023). The Digital Undertow and Institutional Displacement: A Sociomaterial Approach. *Organization Theory*, *4*(2), 1-16.

Radzikowski, P. (2008). 'Reach-Back' - A New Approach To Asymmetrical Warfare Intelligence. *Army*, *58*(12), 24-26.

Renault, C., Charon, P. & Laurençon, F. (2023). Renseigner autrement ? Trajectoires de l'Osint dans les services de renseignement. *Hérodote*, *186*(3), 19-30.

Steel, R. D. (1990). Intelligence in the 1990's: Recasting national security in a changing world. *American Intelligence Journal*, *11*(3), 29-36.

Talamantes, J. (2019). *Physical Red Team Operations*, Hexcode Publishing.

Vest, J. & Tubberville, J. (2019). *Red Team Development and Operations: A practical guide*, Zero-Day Edition.