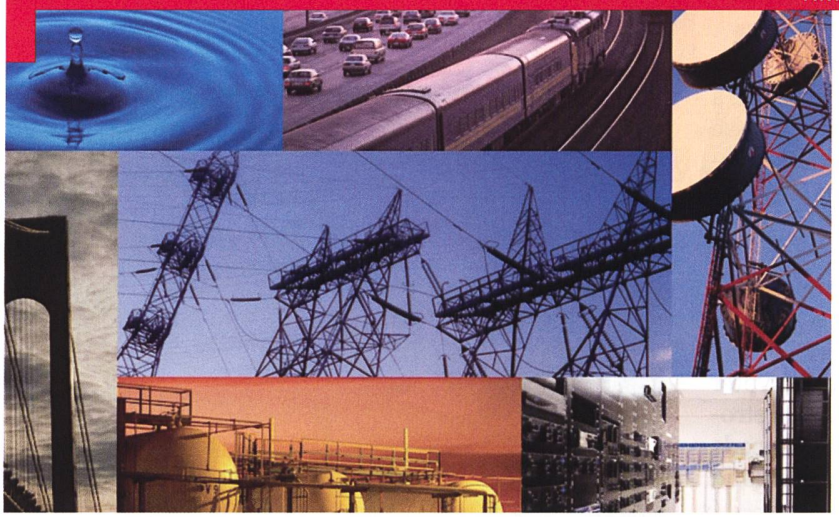
Zeitschrift: Revue Militaire Suisse
Herausgeber: Association de la Revue Militaire Suisse
Band: - (2024)
Heft: 6

Artikel: 2024 : des cyberattaques et du sabotage de la CNI aux cyberconflits internationaux
Autor: Kolochenko, Ilya
DOI: https://doi.org/10.5169/seals-1075573



Cyber

2024 : Des cyberattaques et du sabotage de la CNI aux cyberconflits internationaux

Ilya Kolochenko
Fondateur et CEO de ImmuniWeb

Les conflits dans le cyberespace, y compris les actes hostiles de sabotage et les opérations offensives menées directement par des Etats-nations ou par des cybermercenaires commandés et parrainés par des gouvernements, sont connus depuis près de vingt ans.[1][2] La nature hautement destructrice, la sophistication technique et la préparation minutieuse figurent parmi les caractéristiques des cyber-opérations parrainées par des Etats. Les infrastructures nationales critiques (INC) sont l'une des principales cibles de ces opérations, car leur défaillance ou leur dysfonctionnement maximise les dommages et renforce l'effet psychologique durable de l'opération. Le manuel de Tallinn, élaboré à l'origine par un groupe d'éminents experts techniques, militaires et politiques et de juristes sous la direction du professeur Michael Schmitt, décrit de manière convaincante la question de savoir si les cyber-attaques contre des objets de l'infrastructure nationale critique constituent un acte de guerre, ainsi que la manière de répondre à de telles attaques dans le respect du droit international.[3] Le présent article passe brièvement en revue l'évolution rapide du paysage des cyberopérations offensives menées par des acteurs étatiques à l'encontre de CNI, offre un aperçu succinct de la législation nationale existante et émergente destinée à protéger les CNI et à renforcer la cyberrésilience spécifique à un Etat ou supranationale, et examine de manière concise la possibilité et les implications d'un cyberconflit international majeur dans le contexte des nouvelles capacités techniques des acteurs de la cybermenace, telles que l'IA générative (GenAI).

Aujourd'hui, la définition précise des infrastructures nationales critiques (INC) peut varier d'une juridiction à l'autre, mais la plupart des Etats occidentaux convergent vers une définition globale et inclusive des INC, qui couvre un large éventail d'entités privées et gouvernementales, allant des centrales nucléaires et des barrages hydroélectriques aux institutions financières privées et aux fournisseurs d'accès à l'internet d'une certaine taille. [4][5] Dans le contexte de la crise géopolitique qui se développe progressivement, la cybersécurité des objets CNI est devenue cruciale pour la stabilité et la sécurité des Etats souverains. En avril 2023, le Centre national de cybersécurité du Royaume-Uni (NCSC) a lancé un sombre avertissement concernant les risques sans précédent de cyberattaques étrangères et d'actes de cyber-sabotage à l'encontre des infrastructures nationales britanniques.[6] Plus tard, en février 2024, le message alarmant a été repris par l'Agence américaine de cybersécurité et de sécurité des infrastructures (CISA), qui a souligné les risques de compromission furtive et de piratage sophistiqué d'entités CNI américaines par des acteurs étrangers de la cybermenace.[7] Entre-temps, un rapport mondial sur les ransomwares, publié par Sophos en juillet 2024, a mis en évidence l'état de délabrement de la cybersécurité des ICN et son attrait pour les acteurs de la cybermenace motivés par des considérations financières. Le rapport indique notamment que le montant médian des rançons payées par les entités CNI compromises est passé de 62'500 USD à 2,54 millions USD au cours des 12 derniers mois. [8]

1 Richard Stiennon, "A short history of cyber warfare", *Cyber Warfare : A Multidisciplinary Analysis (1ère éd.)*, Routledge, 2015

2 Dixie O'Donnell, "Geopolitics and Cyberspace", *Geneva Centre for Security Policy (GCSP)* - https://www.gcsp.ch/global-insights/geopolitics-and-cyberspace - 13 décembre 2019

3 Centre d'excellence en coopération pour la cyberdéfense de l'OTAN (CCDCOE), The Tallinn Manual - https://ccdcoe.org/research/tallinn-manual/ - consulté le 8 août 2024.

4 Directive présidentielle américaine (PPD) 21 : Sécurité et résilience des infrastructures critiques - https://www.cisa.gov/resources-tools/resources/presidential-policy-directive-ppd-21-critical-infrastructure-security-and - 12 février 2013

5 Directive européenne 2022/2557 du Parlement européen et du Conseil du 14 décembre 2022 relative à la résilience des entités critiques - https://eur-lex.europa.eu/eli/dir/2022/2557/oj - 27 décembre 2022

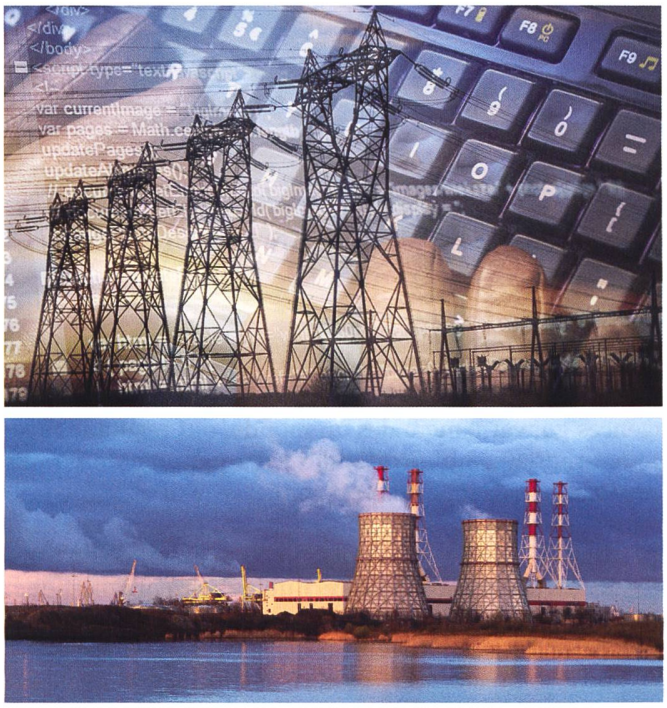
6 UK National Cyber Security Center (NCSC), "NCSC warns of emerging threat to critical national infrastructure", 19 avril 2023 -

7 Agence américaine de cybersécurité et de sécurité des infrastructures (CISA), "PRC State-Sponsored Actors Compromise and Maintain Persistent Access to U.S. Critical Infrastructure" - https://www.cisa.gov/news-events/cybersecurity-advisories/aa24-038a - 7 février 2024

8 Connor Jones, "Ransomware continues to pile on costs for critical infrastructure victims", *The Register* - https://www.theregister.com/2024/07/17/ransomware_continues_to_pile_on/ - July 17, 2024

En revanche, dans la plupart des pays, la législation nationale suit tardivement la spirale des risques liés aux infrastructures critiques, dont l'impact et l'ampleur s'amplifient. Aux Etats-Unis, la loi fédérale CIRCIA (Cyber Incident Reporting for Critical Infrastructure Act), la législation hétéroclite des Etats américains et les réglementations des agences fédérales et des Etats couvrent les aspects fondamentaux de la protection et de la défense des infrastructures critiques, ainsi que les exigences en matière de signalement des incidents. Dans l'UE, la directive sur la résilience des entités critiques, la directive sur la sécurité des réseaux et des systèmes d'information (NIS 2) et la loi sur la résilience opérationnelle numérique (DORA), combinées aux lois nationales des Etats membres de l'UE, régissent la sécurité et la résilience des ICN européennes. En Suisse, la récente modification de la loi fédérale sur la sécurité de l'information (LSI) a introduit l'obligation de signaler les incidents liés aux CNI, qui, au moment de la rédaction du présent document, doit encore être précisée par une ordonnance fédérale à venir.[9] Paradigmatiquement, une part considérable des efforts des législateurs des deux côtés de l'Atlantique se concentre sur la prescription d'un niveau adéquat de cybersécurité et d'obligations de déclaration des incidents, sur l'interdiction des pratiques de cybersécurité inférieures aux normes ou obsolètes, et sur la sanction de la non-conformité, parfois - sévèrement - en incluant des poursuites pénales pour les entités non-conformes.[10] Cela dit, la plupart des exigences de ces réglementations sont comparativement plus souples que, par exemple, l'obligation de déclaration d'incident dans les six heures imposée en Inde à pratiquement toutes les entités nationales, et pas seulement aux opérateurs CNI, bien que certains types d'incidents mineurs soient exclus de la déclaration obligatoire.[11]

La pression croissante exercée par les régulateurs et les législateurs est toutefois justifiée si on la considère sous l'angle des risques et de l'impact dévastateur des cyberattaques contre les ICN. Des campagnes de piratage sophistiquées visant des opérateurs d'infrastructures véritablement critiques, comme l'attaque dévastatrice contre le réseau électrique ukrainien qui a provoqué une coupure de courant pour près de 250'000 personnes[12] ou la célèbre attaque par ransomware contre Colonial Pipeline qui a déclenché une déclaration d'urgence régionale dans 17 Etats américains afin d'atténuer la prolifération des pénuries d'essence et la panique concomitante,[13] illustrent bien à quel point les conséquences de telles attaques peuvent



être graves, dommageables et coûteuses. Il est important de noter que ces attaques ne sont que la partie émergée du gigantesque iceberg de la cybercriminalité d'origine étatique, qui reste largement sous-estimée, voire totalement inaperçue, par de nombreuses institutions et commissions gouvernementales. Pour illustrer ce point, on peut jeter un coup d'œil sur la récente débâcle de CrowdStrike. Une erreur innocente dans une mise à jour logicielle de CrowdStrike - l'une des principales sociétés américaines de cybersécurité - a soudainement, quoique rapidement, transformé plus de 8,5 millions d'ordinateurs dans le monde en briques d'introduction avec ce que l'on appelle l'écran bleu de la mort de Windows, provoquant une perturbation mondiale de nombreuses compagnies aériennes, aéroports et opérateurs ferroviaires, une paralysie massive des institutions financières et de santé, et une panne durable des ressources médiatiques et des chaînes de télévision.[14] Cet incident a mis en évidence de manière éloquente la dépendance profonde, substantielle et pratiquement incurable des entités CNI modernes à l'égard de technologies tierces échappant à leur contrôle. On peut imaginer un incident similaire lorsque la mise à jour d'un logiciel n'est pas seulement défectueuse mais contient un logiciel malveillant destructeur visant à compromettre tous les systèmes voisins et à effacer leurs données. Ce scénario catastrophe peut avoir un effet domino sur des milliers d'opérateurs CNI et entraîner une perturbation colossale des activités dans le monde entier et des pertes de plusieurs milliards de dollars. Il convient de noter que des centaines de grands fournisseurs de technologies de l'information déploient quotidiennement leurs mises à jour sur des millions de systèmes et de serveurs critiques appartenant à des entités CNI, tout en étant eux-mêmes sensibles et vulnérables à des cyberattaques sophistiquées, comme dans l'affaire SolarWinds, où plus de 18'000 clients, dont les plus grandes entreprises et

[9] Conseil fédéral suisse, "Le Conseil fédéral met en consultation l'ordonnance sur la cybersécurité" - https://www.admin.ch/gov/en/start/documentation/media-releases.msg-id-101088.html - 22 mai 2024

[10] Règlement (UE) n° 2022/2554 du Parlement européen et du Conseil du 14 décembre 2022 sur la résilience opérationnelle numérique (DORA), voir les articles 50 à 52.

[11] Argus Partners, "Cert-IN's Six Hour Reporting Rule for Cyber Security Incidents - Statutory Interpretation and Analysis", *Legal 500* - https://www.legal500.com/developments/thought-leadership/cert-ins-six-hour-reporting-rule-for-cyber-security-incidents-statutory-interpretation-and-analysis/ - 25 novembre 2022

[12] Jean-Pierre Hauet, "Ukrainian power grids cyberattack, A forensic analysis based on ISA/IEC 62443", *International Society of Automation (ISA)* - https://www.isa.org/intech-home/2017/march-april/features/ukrainian-power-grids-cyberattack - April, 2017

[13] Jen Easterly et Tom Fanning, "The Attack on Colonial Pipeline : Ce que nous avons appris et ce que nous avons fait au cours des deux dernières années", *US CISA* - https://www.cisa.gov/news-events/news/attack-colonial-pipeline-what-weve-learned-what-weve-done-over-past-two-years - 7 mai 2023

[14] Alex Scroxton, "CrowdStrike update chaos explained : What you need to know", *ComputerWeekly* - https://www.computerweekly.com/feature/CrowdStrike-update-chaos-explained-What-you-need-to-know - 29 juillet 2024

agences gouvernementales du monde, ont reçu une mise à jour antidatée qui proviendrait d'un groupe de pirates informatiques d'un Etat étranger.[15]

En 2024, les opérateurs privés et gouvernementaux des entités CNI devront faire face à un ennemi pragmatique, extrêmement bien préparé et équipé. Au cours de la dernière décennie, l'industrie de la cybercriminalité est passée de groupes désorganisés d'acteurs amateurs de cybermenaces à une industrie formidablement mature avec une division du travail intelligente et économiquement productive ( ). Les gangs de cybercriminels modernes se spécialisent généralement en fonction de critères précis, ce qui leur permet d'atteindre un niveau d'excellence, de rentabilité et d'efficacité technique remarquable.[16] Par exemple, un groupe - qui fait parfois appel aux services professionnels d'auteurs, de psychologues ou même d'avocats involontaires - prépare une campagne d'hameçonnage sur mesure, qui exploite couramment les émotions humaines et les tendances ou événements propres au secteur, et qui peut atteindre un taux de clics de 99 %, même parmi les victimes qui suivent une formation continue en matière de cybersécurité. Le deuxième groupe loue ou compromet des serveurs de messagerie tiers, achète ou détourne des domaines dignes de confiance et teste l'e-mail de phishing sur la solution antispam de la victime pour s'assurer qu'il est délivré sans problème avant de l'envoyer. Le troisième groupe développe des logiciels malveillants de pointe, spécialement conçus pour contourner les contrôles de sécurité multicouches de la victime et pour infecter son appareil ; à ce propos, de nombreuses grandes entreprises divulguent involontairement la pile complète de leurs logiciels et matériels de sécurité dans les descriptions de poste lorsqu'elles publient des offres d'emploi pour leurs équipes de cybersécurité. Le quatrième groupe prend le contrôle à distance de la machine compromise et tente de pivoter en interne, en pénétrant dans le plus grand nombre possible d'hôtes, d'appareils et de serveurs du réseau voisin, en mettant en place des portes dérobées furtives chaque fois que c'est possible. Une fois la persistance dans le réseau interne de la victime terminée, les pirates commencent à exfiltrer silencieusement les données de la victime, tout en restant invisibles aux radars des équipes de cybersécurité : selon le Data Breach Report 2024 d'IBM, la détection moyenne des brèches internes prend 61 jours, tandis que la détection des intrusions dans des environnements plus complexes, comme une infrastructure sur site combinée à un environnement multicloud, prend jusqu'à 258 jours.[17] Enfin, un autre groupe exige le paiement d'une rançon en crypto-monnaie peu traçable, offrant fréquemment une assistance technique vingt-quatre heures sur vingt-quatre dans la langue de la victime, donnant des conseils sur la manière d'acheter des bitcoins ou d'autres moyens de paiement numérique, d'effectuer une transaction test, puis de virer l'intégralité du montant.[18] Il va sans dire que la plupart des entités CNI seront inévitablement victimes de ces cyber-attaques remarquablement bien planifiées, intelligemment orchestrées et savamment exécutées.

Outre la sophistication incessante des tactiques et des techniques de piratage, les progrès récents de la GenAI et la disponibilité généralisée de puissants modèles de langage exacerbent sérieusement la situation. Alors que les cybermercenaires professionnels et les groupes de cybercriminels soutenus par les Etats n'obtiendront probablement que peu ou pas de valeur de la GenAI dans la recherche et la découverte des vulnérabilités dites "zero-day",[19] dans le développement de logiciels malveillants et d'exploits vraiment sophistiqués, ou dans l'exécution de mouvements latéraux dans des réseaux compromis[20] - en raison du manque de données d'entraînement à l'IA de haute qualité et des capacités encore primitives des LLM dans l'exécution de tâches avancées et très compliquées - les LLM fournissent des capacités impressionnantes pour la désinformation, l'usurpation d'identité et les activités connexes.[21] Par exemple, les LLM librement accessibles peuvent facilement générer des posts de médias sociaux impeccablement écrits et dignes de confiance, en usurpant l'identité d'utilisateurs réels, d'entreprises ou d'agences gouvernementales. En outre, les LLM peuvent également générer des images et des vidéos usurpant l'identité de politiciens ou de fonctionnaires d'une manière alarmante et crédible, en imitant parfaitement la voix et l'apparence. En outre, la GenAI peut être exploitée pour copier et reproduire rapidement des sites web gouvernementaux sur des domaines typo-squattés ou cyber-squattés, en étant pratiquement impossible à distinguer des ressources web originales, afin de diffuser des informations erronées ou des logiciels malveillants pour le compte d'une agence gouvernementale.

[15] US Government Accountability Office (GAO), "SolarWinds Cyberattack Demands Significant Federal and Private-Sector Response" - https://www.gao.gov/blog/solarwinds-cyberattack-demands-significant-federal-and-private-sector-response-infographic - 22 avril 2021

[16] Ilia Kolochenko, "Five Reasons Why Law Enforcement Loses the Battle Against Cybercrime", *New York Law Journal* - https://www.law.com/newyorklawjournal/2024/05/29/five-reasons-why-law-enforcement-loses-the-battle-against-cybercrime/ - 29 mai 2024

[17] IBM, "Cost of a Data Breach Report 2024" - https://www.ibm.com/reports/data-breach - 30 juillet 2024

[18] Alfred Ng, "Malware now comes with customer service", *CNET* - https://www.cnet.com/news/privacy/ransomware-goes-pro-customer-service-google-25-million-black-hat/ - 26 juillet 2017

[19] US National Institute of Standards and Technology (NIST), "Zero Day Attack" - https://csrc.nist.gov/glossary/term/zero_day_attack - consulté le 8 août 2024

[20] Alex Scroxton, "AI will heighten global ransomware threat, says NCSC", *ComputerWeekly* - https://www.computerweekly.com/news/366567396/AI-will-heighten-global-ransomware-threat-says-NCSC - 24 janvier 2024

[21] Michael P. Heiskell et Ilia Kolochenko, "Generative AI for Criminal Defense Lawyers : Mythes, risques et avantages", *The Champion® by the National Association of Criminal Defense Lawyers (NACDL)* - https://www.nacdl.org/Article/June2024-FromthePresidentGenerativeAIforCriminalDe - juin 2024

Le concept de "Cyber Pearl Harbor" a été inventé il y a plusieurs dizaines d'années, mais certains experts techniques et juristes se sont montrés assez sceptiques à son sujet, estimant que sa probabilité et son impact étaient tous deux exagérés.[22] [23] Néanmoins, compte tenu de l'escalade progressive de la crise géopolitique et de la multiplication des conflits militaires dans de nombreuses régions du monde, ainsi que des tendances de la cybercriminalité et des développements techniques brièvement évoqués ci-dessus, la création d'un cocktail explosif de cyberguerre en mélangeant des cyberattaques avec des campagnes d'usurpation d'identité et de fausses nouvelles à grande échelle devient tout à fait possible et parfaitement opérationnelle en 2024. Pour paralyser les économies des pays occidentaux pendant plusieurs semaines, il pourrait suffire de compromettre une douzaine de sociétés informatiques suffisamment importantes et de diffuser des mises à jour malveillantes à leurs entreprises clientes. Parallèlement, avec l'aide de la GenAI, de faux sites web et comptes dans les médias sociaux, usurpant l'identité des entreprises informatiques touchées, fourniront des conseils de remédiation erronés et nuisibles afin d'infliger encore plus de dégâts et de rendre irrécupérables les systèmes et les données touchés. En outre, les forces de l'ordre et les organismes gouvernementaux concernés seront également usurpés sur l'internet, diffusant des fausses nouvelles ou publiant de fausses ordonnances visant à amplifier la panique et les dommages financiers et sociaux. Des politiciens et des responsables gouvernementaux dont l'identité aura été usurpée seront également activement impliqués dans la campagne "Cyber Peal Harbor", ce qui entraînera une érosion rapide de la confiance et renforcera la peur au sein de la population. En conséquence, des milliers de civils pourraient se retrouver sans eau, gaz, électricité, transports, Internet et téléphone, soins de santé et services d'urgence, y compris la police. Le pire, c'est qu'une campagne aussi surréaliste, à première vue, ne coûtera probablement que quelques dizaines de millions de dollars américains, soit beaucoup moins qu'une opération militaire classique d'une ampleur et d'un impact comparables. Il convient de noter que, même si les accusations croisées entre Etats et alliances militaires ne manqueront pas, l'attribution fiable d'une telle opération militaire perfide dans le cyberespace sera pratiquement impossible pour des raisons techniques et opérationnelles.

En conclusion, les gouvernements doivent réévaluer d'urgence leur niveau de préparation nationale à des actes de cyberguerre néfastes et hautement sophistiqués qui pourraient soudainement éclater. Les budgets nationaux de cyberdéfense doivent être augmentés de manière significative sans délai, notamment en allouant des subventions aux entités CNI privées qui ne peuvent pas se permettre d'investir suffisamment dans la cyberdéfense en raison

de leurs faibles marges opérationnelles. L'introduction de nouvelles lois, visant principalement à punir les entités non conformes et à exiger une divulgation rapide des incidents CNI, ne fera qu'ennuyer des entreprises déjà surréglementées et n'empêchera probablement pas l'effondrement cybernétique imminent et le chaos qui s'ensuivra. Enfin, l'armée doit commencer à réorienter rapidement sa stratégie, en passant de la guerre traditionnelle à l'état brut à la guerre cybernétique, telle que la cyberdéfense, le cybercontre-espionnage et les opérations offensives dans le cyberespace, qui dissuaderont les adversaires potentiels en envoyant un signal clair que des opérations cybernétiques similaires, voire plus importantes, peuvent être lancées en représailles ou même en réponse préventive à une attaque. Il est essentiel de commencer à planifier et à agir sans plus tarder, sinon il pourrait être trop tard.

I. K.

[22] Sean Lawson et Michael K. Middleton, "Cyber Pearl Harbor : Analogie, peur et cadrage des menaces de cybersécurité aux Etats-Unis, 1991-2016", *First Monday*, Volume 24, Numéro 3 - 4 mars 2019.

[23] Steven Stone, "A 'Cyber Pearl Harbor' is a myth-daily cyberattacks are the real problem", *Fast Company* - https://www.fastcompany.com/90930822/a-cyber-pearl-harbor-is-a-myth-daily-cyberattacks-are-the-real-problem - August 15, 2023