Revue-IRS

Revue Internationale de la Recherche Scientifique (Revue-IRS)

ISSN: 2958-8413

Vol. 3, No. 2, Mars 2025

This is an open access article under the CC BY-NC-ND license.

Le cyber conflit et son impact sur les nations : Un défi moderne pour la sécurité internationale

ELIFA Fehmi

Abstract: Cyber conflict is defined as a series of strategic cyberattacks aimed at a nation state to disrupt or damage its critical infrastructure. The rise of cyberspace has transformed global security issues, impacting various sectors such as the economy, politics and national defence.

Keywords: Cybersecurity; cyber warfare; nations; war; AI

Digital Object Identifier (DOI): https://doi.org/10.5281/zenodo.**14993406**

1 Introduction

Après la fin de la guerre froide et l'émergence de nouveaux concepts tels que la mondialisation, la numérisation et l'intelligence artificielle, le monde est devenu un grand village. Avec cette évolution, un nouveau type de guerre est apparu : La cyberguerre. Les questions qui se posent ici sont :

- C'est quoi le cyber conflit (Cyber warfare) ?
- Quel est son impact sur les nations ?

FORTINET (leader mondial dans le secteur de la cybersécurité) la définit ainsi : « La cyberguerre est une série de cyberattaques stratégiques contre un État-nation, ce qui lui cause un préjudice significatif. Ces dommages peuvent inclure la perturbation des systèmes informatiques vitaux jusqu'à la mort.

La cyberguerre est généralement définie comme un ensemble d'actions réalisées par une nation ou une organisation pour attaquer les systèmes réseau informatiques des pays ou des institutions dans l'intention de perturber, d'endommager ou de détruire l'infrastructure par des virus informatiques ou des attaques par déni de

service. On espère que des outils efficaces d'intelligence des cyber menaces peuvent réduire les dommages causés par ces attaques » [1].

En d'autres termes, Le cyber conflit désigne l'utilisation de technologies de l'information et des communications pour mener des attaques contre des systèmes informatiques dans le but de perturber, de déstabiliser ou de contrôler des infrastructures nationales essentielles. Alors que le monde devient de plus en plus connecté, les menaces issues du cyberespace sont devenues un défi stratégique majeur pour la sécurité des États.

Le cyber conflit ne se limite pas aux enjeux technologiques, car il touche des secteurs importants tels que l'économie, les systèmes politiques, la défense nationale et les droits individuels. Cet article explore l'impact du cyber conflit sur les nations et les stratégies mises en place pour atténuer ces risques.

2 L'évolution du cyber conflit:

Durant les dernières décennies, les conflits armés se concentraient principalement sur des affrontements physiques, mais avec l'avènement d'Internet et des technologies numériques, un nouveau champ de bataille est apparu. Les cyberattaques peuvent se produire à n'importe quel moment et dans n'importe quelle région, ce qui rend leur détection et leurs répercussions particulièrement complexes.

La nature invisible du cyber conflit permet à des acteurs étatiques et non étatiques de mener des attaques sans avoir à engager directement les forces militaires conventionnelles. Ainsi, des pays peuvent être attaqués sans déclaration formelle de guerre, ce qui pose des défis en matière de diplomatie, de droits internationaux et de gouvernance mondiale.

Voici ci-dessous quelques exemples d'attaques informatiques qui illustrent l'évolution des conflits cyber.

En 2010, la cyberguerre a commencé avec **STUXNET** (un ver informatique conçu par la National Security Agency (NSA) et la Central Intelligence Agency (CIA), en collaboration avec l'unité israélienne 8200, dans le but de s'attaquer aux centrifugeuses iraniennes d'enrichissement d'uranium [2]. Il s'agit de la première cyber arme destinée à causer des dommages physiques. **STUXNET** aurait détruit 20 % de ces centrifugeuses.

Puis, entre 2014 et 2016, la Russie a lancé une série d'attaques stratégiques contre l'Ukraine et le *Bundestag* allemand (Le parlement national allemand). Au cours de la même période, la Chine a piraté 21,5 millions de dossiers d'employés, dérobant des informations au Bureau américain de la gestion du personnel.

Enfin, en 2017, l'attaque **WANNACRY** a touché plus de 200 000 ordinateurs dans 150 pays. Cette cyberattaque ciblait les ordinateurs Windows équipés d'un logiciel de rançon. Plus tard la même année, l'attaque **NOTPETYA**, originaire d'Ukraine, a détruit des fichiers, provoquant des dommages estimés à plus de 10 milliards de dollars.

Mais le terme de cyberguerre est apparu pour la première fois dans le livre « La Guerre hors limites », écrit par les militaires chinois *Qiao Liang* et *Wang Xiangsui* en 1999 [3].

3 Les types de cyberattaques et leur impact :

Les cyberattaques peuvent prendre différentes formes, parmi lesquelles on cite :

Les attaques par déni de service (DDoS) : Ces attaques visent à rendre un site web ou un service en ligne indisponible en surchargeant ses serveurs de requêtes. Bien que leur impact soit souvent limité à la perturbation de services non essentiels, elles peuvent avoir des effets dévastateurs sur des infrastructures critiques telles que les banques, les systèmes de communication gouvernementaux ou les réseaux énergétiques.

- **Les intrusions dans les infrastructures critiques** : Par exemple, des centrales électriques, des réseaux de distribution d'eau ou des systèmes de contrôle aérien peuvent être la cible d'attaques. Une telle attaque peut avoir des conséquences dramatiques sur la sécurité nationale et le bien-être de la population.
- **Les attaques sur les données et le vol de propriété intellectuelle** : Ces cyberattaques visent à dérober des informations sensibles, telles que des secrets industriels, des données personnelles ou toute autre information confidentielle. Les entreprises et les gouvernements sont particulièrement vulnérables à ce type d'attaque informatique.
- **Les campagnes de désinformation et de manipulation de l'opinion publique** : Bien que moins techniques, ces attaques utilisent les médias sociaux et les plateformes en ligne pour influencer les élections, semer la discorde et déstabiliser les sociétés. La guerre de l'information est désormais un élément essentiel des cyber conflits.

L'impact de ces cyberattaques peut être profond. Une attaque contre le système énergétique d'un pays pourrait, par exemple, paralyser l'approvisionnement en électricité, avec des conséquences économiques et sociaux majeurs à la clé.

De même, une campagne de désinformation pourrait semer la confusion parmi la population et affaiblir la confiance dans les institutions publiques.

D'après le précédent exposé, comment ces types de cyberattaques peuvent impacter la sécurité des nations ?

4 L'impact sur la souveraineté et la sécurité des nations :

Le cyber conflit soulève ainsi la question de la souveraineté des nations dans un monde interconnecté. Les cyberattaques, souvent perpétrées par des acteurs étrangers, portent atteinte à l'intégrité des systèmes gouvernementaux et économiques. Contrairement aux conflits militaires traditionnels, les cyberattaques ne respectent pas les frontières géographiques et peuvent être attribuées à un État spécifique de manière difficile. Cela rend la réponse diplomatique et militaire plus complexe.

Les États doivent aussi se préparer à la cyberdéfense et à l'intégration de la cybersécurité dans leurs stratégies de défense nationale. Les gouvernements doivent mettre en place des politiques solides pour sécuriser leurs infrastructures critiques et protéger leurs citoyens contre les cyber menaces. Les alliances internationales, à l'image de l'OTAN, commencent à faire de la cybersécurité une priorité stratégique.

Dans ce contexte, l'exemple de l'opération appelé « *Déluge d'al-Aqsa* » peut permettre d'expliquer plus clairement l'impact des guerres cyber sur la souveraineté et la sécurité des nations.

Environ douze minutes plus tard, les systèmes de **CLOUDFLARE** ont automatiquement détecté et atténué des attaques DDoS ciblant les sites web qui fournissent aux populations civiles des informations vitales et des alertes concernant les attaques à la roquette. La figure suivante explique les attaques par DDOS [4] :

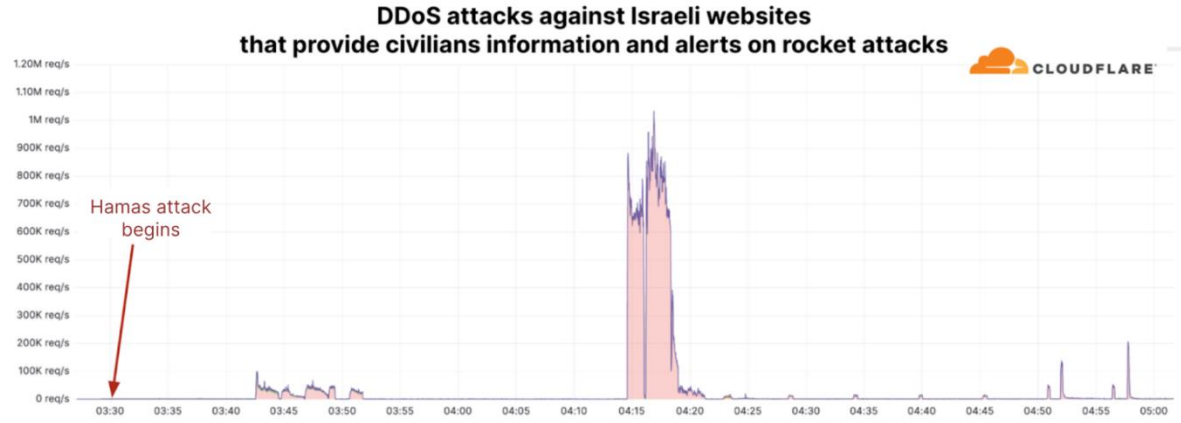

Figure. DDoS attacks against Israeli websites.

Dans le même contexte, on peut également citer le cyber-conflit entre la Russie et l'Ukraine. Il s'agit d'une composante clé de ce conflit. Dès janvier 2022, la Russie a mené des cyberattaques visant à semer la panique en désactivant des sites gouvernementaux ukrainiens, notamment à l'aide du virus **WHISPERGATE** [5]. Ces attaques s'inscrivent dans une continuité remontant à 2013 avec « *opération Armageddon* » [6].

Juste avant l'invasion, des cyberattaques ont ciblé des infrastructures critiques, notamment un fournisseur de satellites américain utilisé par l'armée ukrainienne.

En réponse, l'Ukraine s'est elle aussi engagée dans la cyberguerre, notamment avec « *Opération Prikormka* » dès 2016 [7]. Après l'invasion du 25 février 2022, *Mykhailo Fedorov* (premier vice-premier ministre et ministre de la transformation numérique) a annoncé la création de **L'ARMEE INFORMATIQUE D'UKRAINE**, un effort coordonné pour mener des cyberattaques contre la Russie.

En avril 2022, les autorités ukrainiennes ont également signalé des tentatives de piratage via **TELEGRAM** et des cyberattaques sur des infrastructures électriques [8].

5 La réponse des nations : Stratégies de cybersécurité et de coopération internationale :

Face à cette menace croissante, les pays ont mis en place diverses stratégies de cybersécurité. Elles incluent la création d'agences gouvernementales spécialisées dans la défense cybernétique, le renforcement des législations relatives à la sécurité informatique et l'amélioration de la coopération entre les secteurs public et privé.

La coopération internationale est également essentielle pour lutter contre les cyber conflits. Des initiatives telles que les accords internationaux sur la cybersécurité, la mise en place de normes pour attribuer les cyberattaques et le partage d'informations entre les pays sont cruciales pour gérer cette menace transnationale.

Cependant, ces efforts sont confrontés à des défis, notamment le manque de consensus mondial sur la réglementation du cyberespace et la difficulté de faire appliquer les règles du droit international dans ce domaine.

6 Perspectives futures :

À l'avenir, la cyberguerre continuera de se développer, en particulier avec l'émergence de nouvelles technologies comme l'intelligence artificielle, l'Internet des objets (IoT) et la 5G. Malgré les avantages considérables apportés par ces technologies, celles-ci sont capables de vulnérabiliser les systèmes nationaux.

Les nations devront reconsidérer leur approche de la sécurité nationale pour y intégrer les menaces cybernétiques. L'armement du cyberespace et la création de capacités offensives et défensives seront probablement au cœur des débats géopolitiques.

7 Conclusion:

Le cyber conflit représente en effet un défi majeur pour la sécurité et la souveraineté des nations à l'ère numérique. Les cyberattaques ont des répercussions économiques, politiques et sociales considérables, et les États doivent adapter leurs stratégies de défense en mettant en place des politiques de cybersécurité efficaces. Face à ces menaces globales, la coopération internationale, l'élaboration de normes communes et l'innovation en matière de défense sont des éléments clés pour garantir la sécurité et la stabilité du cyberespace.

Dans ce contexte, il devient impératif que les nations unissent leurs forces pour renforcer leur résilience face aux attaques futures.

REFERENCES

[1] https://www.fortinet.com/fr/resources/cyberglossary/cyber-warfare#:~:text=La%20cyberguerre%20est%20g%C3%A9n%C3%A9ralement%20d%C3%A9finie,attaques%20par%20 d%C3%A9ni%20de%20service.

[2] https://fr.wikipedia.org/wiki/Stuxnet

[3] https://fr.wikipedia.org/wiki/La_Guerre_hors_limites

[4] https://blog.cloudflare.com/fr-fr/cyber-attacks-in-the-israel-hamas-war/

[5] https://fr.wikipedia.org/wiki/Cyberattaque_de_2022_en_Ukraine

[6] Jen Weedon, FireEye, Cyber War in Perspective: Russian Aggression against Ukraine, Tallinn, NATO CCD COE Publications, 2015 (ISBN 978-9949-9544-5-2, lire en ligne [archive]), « Beyond 'Cyber War': Russia's Use of Strategic Cyber Espionage and Information Operations in Ukraine »

[7] Alexey Minakov, « Антивірусна компанія ESET на службі терористів Донбасу » [archive du 16 juillet 2020], Інформнапалм, 1er juin 2016 (consulté le 21 juillet 2020)

[8] James Pearson, Ukraine launches 'IT army,' takes aim at Russian cyberspace, 27 février 2022