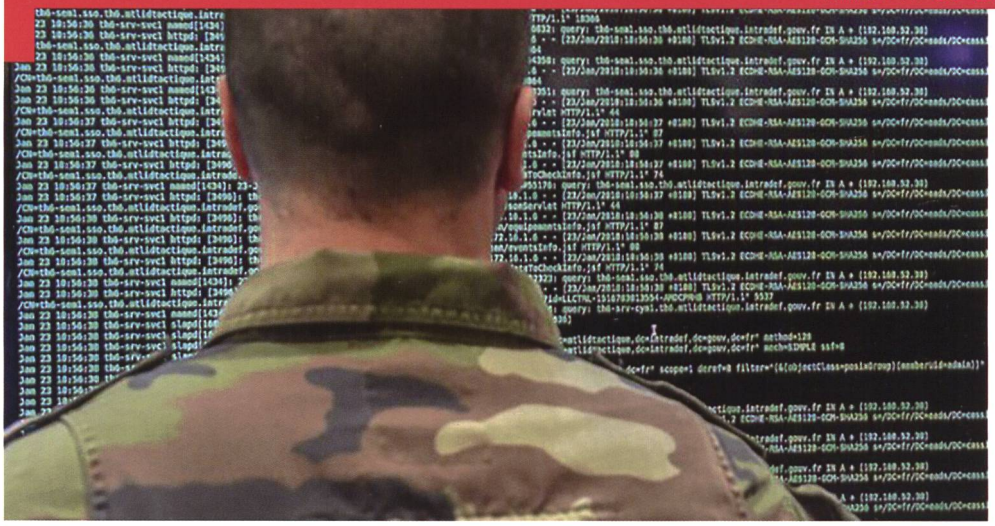
Zeitschrift: Revue Militaire Suisse
Herausgeber: Association de la Revue Militaire Suisse
Band: - (2022)
Heft: 3

Artikel: La première cyberguerre en Europe? : L'anatomie d'un affrontement dans l'espace numérique et les leçons à en tirer
Autor: Helbling, Mirko J. / Ruggli, Oliver / Donon, Yann
DOI: https://doi.org/10.5169/seals-1044744



Cyber

La première cyberguerre en Europe ? L'anatomie d'un affrontement dans l'espace numérique et les leçons à en tirer.

Mirko J. Helbling, Oliver Ruggli et Yann Donon

Depuis la fin de sa formation professionnelle, Mirko J. Helbling B.Sc., MBA, CAS est actif dans le domaine l'informatique et en particulier de la cybersécurité. Il enseigne en à l'école supérieure TEKO de Berne dans le cadre de ses études postgrades « Cybersecurity & Privacy » et de la FFHS. Depuis quatre ans, il travaille dans l'industrie de la défense, en particulier de cryptographie appliquée, de la communication sécurisée ainsi que des architectures pour les systèmes sécurisés en tant que Head Cyber Defence Technologies. Intéressé par la sécurité OT et IoT, il est notamment titulaire de certificats CISSP, CISA, CISM et CEH, ainsi que de diverses formations continues dispensées par en Suisse et à l'étranger.

Oliver Ruggli M.Sc., après avoir obtenu son CFC d'informaticien et acquis de l'expérience dans le domaine des services informatiques au sein d'une entreprise pharmaceutique suisse, a entamé des études d'informatique de gestion et de sciences informatiques à la Fachhochschule Nordwestschweiz (FHNW). Depuis un an, il travaille dans l'industrie de la défense et se concentre sur les thèmes de l'analyse business, des architectures informatiques et des projets d'innovation. Depuis le début de cette année, il approfondit travaille dans les domaines des architectures de sécurité et de l'innovation.

Yann Donon, Ph.D., est Data Science Lead pour l'unité de cyberdéfense de RUAG. Après ses études à Lausanne, il a commencé sa carrière internationale dans l'industrie aérospatiale. Sa thèse de doctorat lui a valu d'être membre d'un institut de l'Académie des sciences de Russie et d'obtenir un poste au CERN. Il y a travaillé comme chercheur principal et a effectué des travaux postdoctoraux dans le cadre de la collaboration DUNE. Ses principaux intérêts de recherche sont la détection et la prédiction d'anomalies appliquées aux domaines de la sécurité des réseaux, de l'imagerie et de l'analyse comportementale.

La cyberguerre actuelle entre l'Ukraine et la Russie n'est pas le premier conflit numérique en Europe ou autour de l'Europe. En revanche, la très forte participation d'entités civiles à l'effort de guerre numérique est impressionnante. Ce « nouveau » mercenariat numérique aggrave le danger émanant des cyberguerres classiques, d'où la nécessité d'anticiper cette menace.

Un changement d'époque ?

Ces dernières semaines, le terme « Zeitenwende » a déjà été mentionné à plusieurs reprises dans le contexte du conflit entre la Russie et son voisin ukrainien. Olaf Scholz, le chancelier allemand, a inventé ce terme en désignant par là un changement de paradigme de la politique de défense allemande le 27 février de cette année. Ce terme pourrait tout aussi bien s'appliquer à l'anatomie du conflit dans le monde numérique. Vivons-nous un changement d'époque dans la guerre numérique ?

Les bases de la cyberguerre

La notion de guerre numérique n'est ni nouvelle ni définie de manière uniforme. Toutefois, avec la numérisation et la dépendance qui en découle, sa pertinence et sa visibilité ont considérablement augmenté au cours des dernières années. D'un point de vue général, la plupart des entreprises forment leurs collaborateurs par le biais de campagnes de sensibilisation ayant une répercussion sur la base dans la société. En outre, certaines personnes ont déjà fait des expériences individuelles, par exemple avec des virus et des e-mails de phishing, et peuvent donc se représenter un peu mieux ces menaces abstraites.

Dans cet article, nous entendons par guerre numérique exclusivement la cyberguerre, qui utilise comme moyen des technologies filaires ou sans fil basées sur des protocoles Internet standardisés (IPv4/IPv6) et qui se déroule donc principalement via Internet. En revanche, la guerre de l'information ne sera pas abordée plus avant.

Un coup d'œil sur l'histoire de la guerre numérique et une vision un peu plus large de la définition permettent de constater rapidement qu'il ne s'agit pas du premier conflit numérique sur ou à proximité du continent européen.

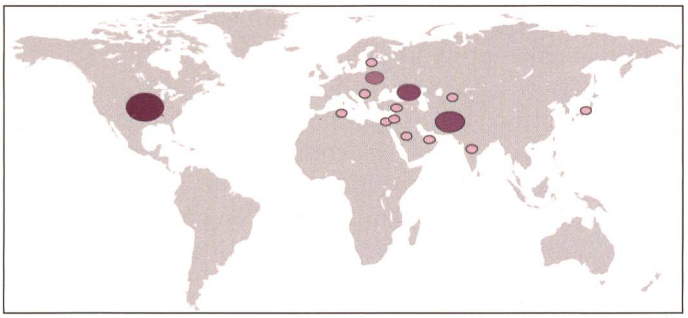


Figure 1: Répartition géographique des principaux événements pouvant assimilés à une cyberguerres.

Les cyber-guerres des dernières années

Dès les conflits des Balkans (1991-2001), la dimension numérique a été utilisée pour mener la guerre, par exemple par l'attaque de membres de l'OTAN par des groupes de pirates informatiques. Lors des conflits qui ont suivi entre la Russie et la Géorgie en 2008, les cyber-attaques ont également pu être constatées comme faisant partie de la conduite de la guerre. En effet, des attaques par déni de service distribué (DDoS) ont été lancées contre des serveurs gouvernementaux, suivies en parallèle des premières attaques d'artillerie et aériennes; d'un point de vue historique, il s'agissait de la première cyberattaque coordonnée avec des moyens de combat classiques. D'autres actions similaires à des guerres dans l'espace numérique ont été constatées lors de la deuxième révolution des tulipes au Kirghizstan en 2009 ainsi que lors de la révolution du jasmin qui a suivi en Tunisie. Au début du conflit dans le sud et l'est de l'Ukraine en 2014 et 2015, on a également pu observer des attaques à la fois graves et extrêmement complexes contre des infrastructures critiques de l'Ukraine. Ainsi, les technologies d'exploitation, c'est-à-dire principalement les systèmes SCADA nécessaires à l'exploitation du réseau électrique, ont été attaquées. On soupçonne généralement un acteur étatique d'être à l'origine de telles attaques, qui ont souvent un motif politique et présentent en outre une grande complexité. Ces dernières années, on a pu observer un renforcement massif des moyens et des méthodes dans le domaine de la cyberguerre de la part des grandes puissances militaires que sont les Etats-Unis, la Russie et la Chine.

Les structures étatiques derrière les cyberguerres

Pour étudier les capacités qui pourraient être mises en œuvre dans le cadre d'une guerre numérique, il convient d'examiner les structures étatiques qui mettent à disposition les moyens et les méthodes correspondants. En ce qui concerne la puissance hégémonique occidentale que sont les Etats-Unis, une part importante de la force de frappe numérique se trouve dans la *communauté du renseignement*, c'est-à-dire dans les services de renseignement étatiques. La National Security Agency (NSA) sert de prestataire de services de télécommunication et de renseignement, dirigé conjointement avec le *Cyber Command militaire américain* Cybercom. Les capacités opérationnelles principales sont assurées par le *Tailerd Access Operations Group (TAO)*, une unité organisationnelle chargée des opérations numériques spéciales de la NSA, à qui l'on attribue une grande compétence ainsi qu'une certaine proximité avec le *Equation Group*. Groupe de pirates informatiques dont l'existence a été révélée en 2016 par l'entreprise de sécurité russe Kaspersky Lab.

En outre, la Central Intelligence Agency (CIA) ainsi que le Department of Homeland Security (DHS) et le Federal Bureau of Investigation (FBI) ont également renforcé leurs capacités, généralement en étroite collaboration avec le secteur privé.

La Russie poursuit en revanche un développement asymétrique des capacités dans la sphère d'opération cyber. Après la dissolution des services secrets soviétiques (KGB), quatre organisations ont été créées. Le *FSO* pour la protection du président, le *FSB* comme service de renseignement intérieur et le *SWR* comme service

Figure 2: Représentation d'événements importants pouvant être compris dans le contexte des cyberguerres.

de renseignement extérieur, tandis que les capacités de renseignement militaire sont couvertes par le *GRU*. Du point de vue occidental, les capacités de la Russie reposent sur un mélange entre structures étatiques et criminelles. Ainsi, certains états occidentaux partent du principe qu'une grande partie des APT (par ex. APT28 et APT29) ainsi que le *groupe Waterburg / Turla*, l'*Energetic Bear / Dragonfly* et le *groupe Sandworm / Quedagh* sont contrôlés par l'un des services d'état et donc de la Fédération de Russie. APT est l'abréviation de Advanced Persistent Threat (menace persistante avancée) et décrit une cyberattaque aux conséquences souvent importantes et d'une grande complexité. Les groupes généralement inconnus soupçonnés d'être à l'origine de ces attaques ont ensuite été baptisés APTx, où x est un nombre croissant. Tous ces groupes sont connus pour leurs opérations de grande envergure liées à l'espionnage, à la manipulation d'élections ou à d'autres attaques contre des infrastructures critiques.

Cette circonstance rend extrêmement difficile la différenciation entre la criminalité et les opérations ordonnées par l'Etat russe.

Un essaim masqué et d'autres opportunistes

Parmi tous les groupes de hackers mentionnés précédemment, un nom se distingue auprès du public: *Anonymous*. *Anonymous* a été fondé en 2003 et est souvent présenté, à tort, comme une organisation structurée portant le « masque de Guy Fawkes ». A la question *« qui se cache derrière le masque »*, l'organisation elle-même donne la réponse: « Toute personne qui soutient nos actions à un moment donné ». Le 24 février 2022, l'un des *principaux comptes Twitter* du groupe a déclaré la *« cyber-guerre contre le gouvernement russe »*. Cette cyber menace est en fait un groupe d'individus possédant des connaissances informatiques de base, qui ne sont généralement pas liés à un gouvernement ou à une organisation structurée (bien que l'on puisse supposer que des acteurs étatiques ont récemment infiltré ces collectifs). Au lieu d'attaques menées ou coordonnées sur une infrastructure donnée, on peut imaginer un essaim tenté de piller un « territoire ». Depuis le 24 février 2022, des centaines d'attaques de ce type ont été documentées contre la Russie, qui auraient paralysé des médias ainsi que le site web du ministère russe de la Défense, publié des contenus internes d'entreprises privées liées à la Russie dans l'industrie militaire et la banque centrale russe, ou envoyé des messages personnalisés sur le conflit.

Ce modus operandi est facilité par la réduction de la complexité technique du piratage. Des études récentes ont mis en évidence la possibilité d'acquérir des programmes malveillants prêts à l'emploi pour des prix inférieurs à 10 $. Avec ces produits, il est possible pour toute personne ayant des connaissances de base en informatique de participer à des attaques. Actuellement, on suppose que la mise à disposition de ces produits au grand public fait partie de la stratégie de cyberguerre de certains Etats. En revanche, le seul fait confirmé est qu'*Anonymous* a déclaré la « *guerre numérique* » à l'Etat russe et constitue donc, du moins en apparence, un belligérant autonome aux côtés de l'Ukraine. Cette circonstance permet d'observer une cyberguerre supranationale.

Guerre actuelle dans l'espace numérique

Dans une cyber-guerre comme celle-ci, il existe des modèles d'attaques opportunistes et ciblées qui peuvent être observés.

Les attaques opportunistes ont pour but d'infliger des dommages « quelconques » à l'adversaire ou à des organisations liées à l'adversaire, indépendamment d'une compréhension profonde de la stratégie.

Les collectifs de hackers indépendants comme *Anonymous* ou d'autres combattants solitaires, les « loups solitaires », appartiennent à ce genre, dans la mesure où ils évaluent ou prennent en charge des cibles en fonction de leurs sentiments et de leurs opinions. En revanche, les attaques ciblées sont souvent menées par des organisations gouvernementales qui choisissent les cibles dans le cadre d'une stratégie prédéfinie et les infiltrent en conséquence.

L'impact des cyber-guerres et leur utilité pratique sont encore difficiles à évaluer et à prédire, en particulier lorsque les éléments opportunistes font partie intégrante de la tactique. Alors que le GRU tentait en février de s'attaquer aux services administratifs et aux infrastructures critiques par le biais d'attaques DDoS afin de limiter leur disponibilité, divers groupes de pirates russes ont répliqué en lançant d'autres attaques DDoS contre le ministère ukrainien de la Défense par le biais de DanaBot, une plate-forme de *malwares as a service*. Parallèlement, diverses attaques *Wiper* ont été détectées, qui présentaient toutes un schéma similaire. Depuis le début de l'année, différents programmes malveillants de *type wiper ont été* détectés sur les systèmes ukrainiens sous les noms de *WhisperGate*, *HermeticWiper*, *Double Zero*, *IsaacWiper* et *CaddyWiper*. Le terme Wiper désigne un programme malveillant, effaçant des données. De tels programmes malveillants sont conçus pour effacer tout ou partie du disque dur de l'ordinateur infecté. Les indices pointent vers une participation du groupe *Sandworm*. *APT28 s'est* également manifesté par une vaste campagne de phishing visant le groupe de médias UKRNet. En outre, au début de l'escalade, le groupe de satellites ukrainien *Visat Outage a été* victime d'une action étendue de la part de la Russie, ce qui a entraîné de graves restrictions dans le domaine des communications du côté ukrainien. Les campagnes ont été accompagnées d'attaques d'espionnage latentes, comme par exemple la porte dérobée *Cameradon*. Il n'est pas encore possible de dresser un tableau définitif de la situation, mais les efforts déployés par la Russie témoignent d'une longue phase de préparation et d'infiltration, ainsi que d'une intention tactique claire au travers des cyberattaques. Nombreux sont ceux qui pensent que la Russie tente de limiter de manière très granulaire les communications tactiques des forces ukrainiennes et qu'elle lance des actions parallèles pour lier l'armée informatique adverse.

D'un autre côté, un corps d'armée cyberguerre ukrainien s'occupe de tâches défensives, tout en encourageant *les hacktivistes* du monde entier à mener des activités offensives, ce qui a également fait entrer *Anonymous* dans le jeu. *Les hacktivistes* sont généralement des *pirates informatiques* motivés par la politique ou l'idéologie, qui manifestent leur protestation par des actions numériques. Ces attaques opportunistes, qui sont souvent non ou mal coordonnées et dont l'effet tactique est limité, ne présentent un potentiel de danger que par leur quantité et la possibilité d'un coup de chance qui en résulte. Les sanctions imposées au secteur high-tech, qui concernent par exemple la livraison de mises à jour et de correctifs de sécurité, augmentent de manière artificielle la surface d'attaque contre la Russie. La combinaison de plusieurs milliers de *hacktivistes* cherchant à faire fortune sur le réseau russe et tombant sur des systèmes de moins en moins sécurisés, alors que les poursuites judiciaires sont réduites dans l'hémisphère occidental, par rapport aux délits numériques en Russie, complique la situation pour les spécialistes informatiques russes.

Un dangereux programme malveillant *Wiper* visant la Russie, *RURansom, a* également été découvert. Les dirigeants russes ont réagi en prenant des mesures radicales dans le domaine de l'Internet et en promouvant le *Runet*, un Internet spécialement développé pour la Russie, afin de limiter au maximum les dommages.

Les sanctions dans le secteur de la haute technologie, combinées à l'orchestration de *hacktivistes* via corps d'armée cyberguerre ukrainien, poursuivent clairement une stratégie *de défense contre les attaques* en essayant de retenir les spécialistes informatiques russes dans des activités défensives et de limiter ainsi leurs capacités et leur marge de manœuvre.

Conclusions

Contrairement à l'idée reçue, les cyberguerres ne sont que partiellement l'affrontement direct entre deux acteurs contrôlés par l'Etat. Souvent, les entités les plus diverses sont impliquées et des institutions civiles sont au centre des opérations. La combinaison d'actions de guerre économique et d'affrontements numériques de grande ampleur comporte des risques et a le potentiel de dénumériser une société à moyen terme. Les conséquences sociales et économiques qui en résultent pour un Etat sont évidentes. Une certaine indépendance de l'économie et la promotion de la *souveraineté technologique*, c'est-à-dire la compétence en matière de développement, de production et de distribution, permettent de lutter contre ce phénomène. En outre, les structures civiles et militaires doivent être mieux synchronisées dans le domaine de la cybersécurité afin de permettre une réaction coordonnée en cas d'urgence.

M. H., O. R. & Y. D.

Art	Utilisation
Faux signaux/données	GPS Spoofing – Utiliser de faux signaux GPS pour superposer le bon.
Réseaux de zombies	Perturber un appareil ou un réseau cible avec des demandes provenant d'appareils pris en charge – attaque par déni de service distribué (DDoS).
Logiciels malveillants	Programmes qui reposent sur l'ordinateur jusqu›à un certain moment pour devenir actifs en même temps.
Wiper	Programmes qui suppriment les fichiers sur les cibles infectées.
Ransomware	Programmes qui chiffrent les fichiers sur les appareils infectés. Avec le cryptage, les cibles sont souvent invitées à décrypter après avoir payé une rançon.
Fuzzing	Une attaque par fuzzing est un processus automatisé au cours duquel de grandes quantités de données aléatoires (fuzz) sont envoyées à des puces afin de découvrir ou de désactiver des failles de conception.
Bricking	Le bricking désigne un appareil électronique endommagé au point de ne plus pouvoir être réparé, ce qui le rend totalement inutilisable, souvent en raison d'un micrologiciel corrompu.
Hameçonnage	Utiliser des techniques d'ingénierie sociale pour tromper une personne ou un groupe afin d'obtenir des informations de toutes sortes.