L'Ukraine, un allié essentiel à la protection du territoire numérique américain

Jonathan Guiffard[1]

Le 13 avril 2022, les autorités américaines[2] annoncent la découverte du piège informatique (*malware*) Pipedream, conçu pour infecter les infrastructures industrielles américaines. Ce *malware*, identifié par des acteurs américains avant qu'il ne soit activé, a été rendu public le lendemain de l'annonce par la société de cybersécurité ESET de la découverte dans le réseau énergétique ukrainien d'un *malware* très similaire surnommé Industroyer2[3].

Depuis le début de la guerre russe en Ukraine, à partir de février 2014, le gouvernement américain observe un accroissement significatif des opérations russes dans l'espace numérique. Le conflit a servi de terrain d'action et d'entraînement des capacités cyber offensives et informationnelles russes. Ces mêmes outils ont été utilisés dans le territoire numérique américain, avec quelques succès majeurs et traumatisants pour les responsables politiques : l'opération de *hack and leak* contre le Parti démocrate et l'ingérence informationnelle dans le processus électoral national américain en 2016, la pénétration des administrations américaines *via* l'attaque contre la société Solarwind en 2020 et la mise à l'arrêt d'infrastructures énergétiques américaines *via* l'attaque contre la société Colonial Pipeline en 2021.

Le géographe Yves Lacoste définit une représentation géopolitique comme « une construction, un ensemble d'idées plus ou moins logiques et cohérentes »

1. Senio Fellow à l'Institut Montaigne. Doctorant à l'IFG Lab université Paris-8.

2. Dans un communiqué signé par le Département de l'énergie, le *Cybersecurity and Infrastructure Security Agency* (CISA), le FBI et la NSA.

3. Rapport « Industroyer2 and INCONTROLLER », *Vedere Labs & Eindhoven University of Technology, Forescout Technologies, Inc*, 2022, <https://www.forescout.com/resources/industroyer2-and-incontroller-report/>, consulté le 14/04/2023.

Hérodote, n° 190-191, La Découverte, 3e et 4e trimestres 2023.

[Lacoste, 1993]. Cette notion permet aux acteurs d'un conflit de « décrire une partie de la réalité de manière plus ou moins exacte [...] [ce] qui leur permet d'appréhender leur environnement et d'agir dessus, en lui donnant un sens » [Cattaruzza et Limonier, 2019]. Le conflit russo-ukrainien est ainsi l'objet de représentations conflictuelles par les acteurs impliqués, notamment américains, ukrainiens ou russes. Ces lectures rivales déterminent leurs manières d'appréhender un territoire et leurs stratégies pour le façonner. Ainsi, l'Ukraine a rapidement été considérée par les responsables politiques et sécuritaires américains comme un territoire d'intérêt pour la lutte contre les opérations cyber offensives et informationnelles russes. Les politiques de soutien des gouvernements américains au profit des institutions et forces armées ukrainiennes, depuis 2014, illustrent cet engagement, notamment dans le domaine cyber.

Ainsi, les gouvernements des présidents Obama (2013-2017), Trump (2017-2021) et Biden (2021-) ont mis en œuvre, depuis 2014, dans le prolongement direct de la conquête militaire de la Crimée par les forces armées russes, une stratégie de soutien indirect aux institutions ukrainiennes, dans laquelle le partage de renseignement technique et l'appui dans le domaine cyber tiennent une place importante. Les relations stratégiques nées de cette étroite alliance cyber dessinent en creux les objectifs de ces deux acteurs : un accroissement de la surveillance de l'espace numérique pour le gouvernement américain et un renforcement de l'autonomie stratégique pour le gouvernement ukrainien.

Cet article s'appuie sur un terrain de recherche effectué à Washington, en février 2023, dont l'objectif visait à comprendre les facteurs qui influencent les représentations et les stratégies des acteurs cyber américains à l'égard de l'Ukraine. Il s'appuie sur un raisonnement autour de deux axes. Je décrirai l'architecture du soutien fourni par les Américains aux Ukrainiens en montrant que cette politique est favorisée par une position de domination de l'espace numérique par les États-Unis, dont l'agence de renseignement technique et cyber, la National Security Agency (NSA), et l'écosystème industriel sont les acteurs de pointe. Puis je mettrai en lumière les effets de dépendance stratégique mutuelle qui en découlent pour les deux partenaires.

L'écosystème cyber américain s'implante durablement à Kiev

Le choix américain d'un soutien central en renseignement et en cyber

Dès l'automne 2021, la nécessité d'un large partage de renseignement s'est imposée aux acteurs américains car il permettait aux forces armées ukrainiennes de rétablir un rapport de forces favorable face à une armée russe supposée plus

Hérodote, n° 190-191, La Découverte, 3e et 4e trimestres 2023.

forte. Des responsables américains confirment la nature et l'ampleur du soutien en renseignement évoqué dans la presse américaine, après le déclenchement de l'invasion russe de grande ampleur, le 24 février 2022, mais tendent à le relativiser[4]. La presse américaine évoque ainsi un soutien considérable en imagerie satellite (IMINT), en interception du signal et des communications (SIGINT) et dans le ciblage des unités militaires russes. Plusieurs enquêtés confirment ce soutien technique, complémentaire des capacités ukrainiennes dans le domaine du renseignement d'origine humaine (HUMINT). Le directeur du renseignement militaire américain, général Scott Berrier, parle d'un échange de renseignement « révolutionnaire » et le général Nakasone, directeur de la NSA, indique que « durant trente-cinq ans de carrière, il n'avait jamais vu un meilleur partage de renseignement, aussi précis, ponctuel et actionnable »[5].

Cette stratégie de soutien indirect se matérialise singulièrement dans le domaine cyber, en raison de sa dimension renseignement, mais aussi en raison d'un intérêt mutuel ukraino-américain pour la compréhension et la neutralisation de la menace cyber russe. L'appui américain en cyber à l'Ukraine a commencé en 2014 et a été particulièrement stimulé par les cyberattaques de 2015 contre les infrastructures énergétiques ukrainiennes. L'Ukraine a constitué un terrain d'observation et d'analyse de la menace cyber particulièrement riche pour les acteurs institutionnels et privés américains. La NSA et le commandement militaire en charge de la composante cyber qui lui est associé, l'US Cyber Command (CYBERCOM), ont eu intérêt à développer des partenariats étroits avec des alliés soumis aux cyberattaques russes pour les étudier conjointement. Ce choix s'est fait en cohérence avec la stratégie cyber du Département de la défense (DoD), notamment la doctrine d'engagement persistant mise en œuvre dans le cadre de la stratégie nationale cyber de 2018. Cette doctrine est un écho dans l'espace numérique de plusieurs aspects du style national américain, concept qui évoque « la façon dont [la] personnalité collective [d'une Nation] réagit à son milieu et agit sur lui ». Celui-ci est empreint d'exceptionnalisme et d'ethnocentrisme, des traits qui amènent la nation américaine à percevoir sa place et son destin différemment des autres nations et les gouvernements américains à concevoir une vision paranoïaque et messianique des relations internationales. Ainsi, la nation américaine doit protéger son expérience démocratique unique et promouvoir son modèle, amenant ses responsables politiques à développer des stratégies de surveillance et

4. Entretien anonyme avec un responsable de la sécurité nationale, Washington, le 14 février 2023.

5. Audition du 17 mars 2022 par le sous-comité du renseignement des forces armées de la Chambre (House Armed Services subcommittee on intelligence) voir <https://www.youtube.com/watch?v=sr54QBU2lBc&t=1s>, consulté le 5 août 2023.

de protection hors des frontières dans l'objectif de prévenir des menaces lointaines mais orientées contre elle [Balthazar, 2022].

Enfin, à la lumière de l'ingérence russe dans le processus électoral de 2016 et en observant la multitude d'opérations informationnelles dans l'espace numérique ukrainien depuis 2014, les autorités américaines ont fait le choix d'intégrer cette dimension dans leurs doctrines défensives et de s'impliquer pour répondre aux campagnes russes. Cette évolution institutionnelle a favorisé un engagement américain en soutien des Ukrainiens.

Des raisons de la surveillance de l'espace numérique : une menace russe stratégique

La NSA met en œuvre une stratégie pour accroître son territoire de collecte de renseignement technique, afin de répondre à des menaces stratégiques internationales comme l'illustrent ses représentations de la menace russe. Dès le départ de la constitution d'une politique SIGINT en temps de paix, en 1946-1947, le gouvernement américain estimait faire face à une menace soviétique globale qui nécessitait un jeu d'alliances et une implantation territoriale en différents points de la planète. Cette logique persiste aujourd'hui : l'action des autorités russes est scrutée dans son espace régional (Europe de l'Est, Caucase, Asie centrale), mais aussi en Syrie, en Libye et désormais en Afrique sub-saharienne. Les archives diffusées par Edward Snowden confirment que la Russie est restée, après la guerre froide, une cible stratégique de la NSA, longtemps avant le sursaut de la classe politique américaine en 2016 (ingérence électorale). L'amiral Mike Rogers, directeur de la NSA et du CYBERCOM entre 2014 et 2018, confirme que, si les cercles politiques américains ont baissé leur vigilance à l'égard de la Russie dans les années 1990-2000, la NSA n'a jamais arrêté de considérer la Russie comme un adversaire prioritaire à surveiller. Il précise que si la lutte contre le terrorisme a absorbé de nombreuses ressources de la NSA, elle n'en a pas pour autant affaibli la surveillance de la Russie :

> Du point de vue du renseignement, nous avons toujours été préoccupés par ce comportement [russe]. J'ai vu un espionnage intensif contre nous. En 2016, ils ont tenté de manipuler l'élection. On y a mis beaucoup d'attention aussi à cause de notre histoire [commune] [...]. On n'a jamais quitté cette nation de l'œil. Ils ont des cyber-capacités, d'importantes capacités d'espionnage et des capacités militaires. Ils considèrent l'OTAN comme leur principal ennemi [...]. Nous étions très à l'aise avec notre renseignement. Nous avions un volume important de renseignements en 2016 [pour caractériser l'ingérence russe]. En 2021, nous avons rendu publiques des informations issues d'accès soutenus et de haut niveau. Disons d'un niveau assez

Hérodote, n° 190-191, La Découverte, 3e et 4e trimestres 2023.

> élevé. Cette connaissance n'était pas totalement parfaite [...]. [Le flux de renseignements] n'était pas une montagne russe mais un [flux] constant[6].

La coopération étroite avec l'Ukraine s'inscrit ainsi dans les stratégies historiques de la NSA de constitution d'alliances, dont l'objectif vise à étendre sa collecte de renseignement et sa capacité d'action dans l'espace numérique. Pour cette raison, la NSA entretient une large panoplie de relations bilatérales d'échange, de coopération et de mutualisation avec des partenaires plus ou moins privilégiés (14 Eyes ; Third partners ; Tier B) [Pétiniaud, 2014], tout en animant des alliances SIGINT spécifiques à l'image du Senior Sigint Europe (SSEUR) ou du Senior Sigint Pacific (SSPAC) qui sont des forums d'échange régionaux[7]. Ainsi, les documents Snowden permettent de comprendre que par leur proximité avec la NSA ou par les emprises de la NSA qu'ils hébergent sur leur sol, certains pays apparaissent déterminants pour renseigner sur la Russie, notamment l'Allemagne, la Suède, la Turquie et le Danemark. Cette stratégie historique de partenariat de la NSA et du CYBERCOM a naturellement intégré l'Ukraine comme une nouvelle pièce de son dispositif. La NSA a développé des relations étroites avec les différents services de renseignement ukrainiens (SBU, SZRU, GUR). Illustration de l'importance de ce partenariat pour la NSA, elle n'en a jamais parlé à ses alliés européens habituels avant l'invasion du 24 février 2022. Si les responsables de la NSA se montraient volubiles sur leur stratégie générale en Europe de l'Est, ils n'ont jamais évoqué ce partenariat spécifique jusqu'à sa médiatisation forcée par l'invasion[8].

6. Citation originale (traduite par l'auteur) : *« From an intelligence perspective, we were always concerned with that behavior. I saw extensive espionage against us. 2016, they tried to manipulate the election. We put a lot of attention too because of our history [...]. We never took an eye from this nation. They have cyber capabilities, major espionage capabilities and military capabilities. They identify NATO are their key enemy [...]. We were very confortable with our intelligence. We had a large amount for 2016. In 2021, we publicly disclosed insights into our sustained and high level access. Fairly high level. That knowledge was not totally perfect [...] [The stream of intelligence] was not a roller coaster but constant. »* Entretien en ligne avec l'amiral Michael Rogers, ancien directeur de la NSA et de l'US Cyber Command (2014-2018), le 3 mars 2023, Washington DC.

7. « NSA's Foreign Partnerships », *Electrospace.net*, 04/09/2014, <https://www.electrospaces.net/2014/09/nsas-foreign-partnerships.html>, consulté le 22/04/2023.

8. Entretien anonyme avec un ancien directeur d'un service de renseignement français, Paris, le 23 mars 2023.

Un soutien américain présenté comme déterminant

S'il est difficile d'en mesurer l'efficacité dans le cyberespace et dans la guerre, le dispositif de soutien américain joue un rôle essentiel dans le rapprochement entre les gouvernements américain et ukrainien et dans la montée en capacité des Ukrainiens dans les domaines cyber et du renseignement.

Cette coordination travaille à la mise en place d'infrastructures numériques robustes et résilientes. Pour la dimension civile, le Département d'État (DoS) apporte une assistance dans le domaine cyber pour protéger les systèmes économiques, notamment le secteur bancaire. Le DoS soutient aussi budgétairement et politiquement les opérations d'assistance de l'USAID qui, en plus de la construction d'infrastructures, s'est chargé, avant février 2022, de piloter des projets de sensibilisation au risque cyber des entités privées ukrainiennes. En outre, le gouvernement américain aide le président Zelensky à renforcer le State Service of Special Communications and Information Protection of Ukraine (SSSCIP), administration en charge de la politique publique cyber, avec des outils et des ressources budgétaires[9] *via* son homologue américain, le CISA, qui gère le pilotage et le JCDC[10] qui partage des détails techniques issus des entreprises et agences gouvernementales américaines avec les Ukrainiens presque tous les jours[11].

Pour la dimension militaire, l'assistance américaine dans les domaines du cyber et du renseignement est active de longue date. Un ancien responsable du commandement cyber de l'armée de terre (ARCYBER) décrit le contexte qui a façonné cette coopération originale, à partir de cultures opérationnelles différentes :

> Surtout après 2014, les relations entre l'Ukraine et les États-Unis se sont sensiblement développées. Premièrement, en passant par les gouvernements et leurs relations, mais aussi en passant par des entités commerciales (fournissant des éléments non classifiés). En étroite collaboration avec Microsoft, nous travaillons avec eux pour être sûrs que les informations soient transmises aux Ukrainiens. Les renseignements [de la NSA et du Cybercom] ont été transmis à des entreprises américaines, partagés aussi avec d'autres États, qui ont accepté de transmettre ces renseignements aux Ukrainiens [...]. Notre relation avec l'Ukraine est suffisamment mûre pour atteindre un bon niveau de confiance. Elle a mûri mais pas assez vite pour avoir une relation étroite sur des sujets très classifiés. Beaucoup de choses sont déjà partagées avec les

9. Entretien anonyme avec deux experts en cybersécurité, en entreprise, Washington, le 17 février 2023.

10. Joint Cyber Defense Collaborative, centre de coordination cyber du Département de la sécurité nationale (DHS).

11. Échange par mail avec une responsable du bureau des affaires extérieures du Cybersecurity and Infrastructure Security Agency (CISA), le 8 mars 2023.

Hérodote, n° 190-191, La Découverte, 3e et 4e trimestres 2023.

> sociétés de cybersécurité. [Toutefois,] nous n'avons partagé aucun objectif en Russie. Nous avons vu [l'APT] Sandworm ou d'autres types d'unités, nous avons mené [seuls] une opération. Nous avons informé des entreprises américaines des vulnérabilités et des attaques potentielles qui visaient l'Ukraine [pour qu'elles en informent les Ukrainiens]. Par exemple, deux semaines avant la guerre, on a vu venir les capacités [cyber] russes [en Ukraine] [...]. Mais le partenariat n'est pas encore à son meilleur niveau. Si nous partageons des informations classifiées, nous voulons nous assurer qu'elles ne seront pas divulguées. Ils n'ont pas le genre d'infrastructure nécessaire pour nous rassurer : ni la sécurité physique ni la cyber sécurité [...]. Une erreur peut compromettre notre accès[12].

Malgré cette méfiance structurelle, les échanges sont réguliers, denses et variés L'amiral Rogers décrit le soutien apporté par la NSA en particulier :

> Le partenariat avec l'Ukraine commence en 2014, avec la Crimée, qui est un signal d'alarme pour les Ukrainiens. Ils comprennent qu'ils doivent améliorer leur jeu. Ils avaient une très bonne attitude. Ils voulaient écouter, apprendre. Ce fut un effort soutenu. Ce n'était pas « un soutien de 6 mois et puis une autre priorité alors nous partons ». Non, c'était un effort soutenu, un niveau de coopération maintenu au cours des 8 dernières années [...]. Les Ukrainiens sont bons. Ils ne partaient pas de zéro. Ils étaient intelligents et ils avaient des capacités. De très bonnes capacités[13].

---

12. Entretien par appel vidéo avec le colonel Chad Bates, instructeur à l'US Army War College sur les questions cyber et informationnelle, ancien responsable de l'US Army Cyber Command (ARCYBER), le 16 février 2023. Citation originale (traduite par l'auteur) : *« Especially after 2014, the relationship between Ukraine and the US steadily grown. First, working through government and their relationship, but also working through commercial entities (providing unclassified elements). Closely with Microsoft, we work with them to be sure that info were pushed to the Ukrainian. Intelligence were pushed through US companies, shared with other states who agreed to push these intel to Ukrainians [...]. Our relationship with Ukraine is matured enough to attain a good level of trust. It matured but not that quickly to have a close relationship on very classified matters. A lot of stuff are already shared with cyber security corporations. We have not shared any targets in Russia. We see Sandworm or other type of unit, we conducted operation. We tipped off these people, American companies, on vulnerabilities and potential attacks that come for Ukraine. For instance, two weeks before the war, we saw ussian capabilities coming [...]. But the partnership is not at its best level yet. If we share classified information, we want to be sure that it is not leaked out. They do not have that kind of infrastructure to confort us neither the physical security, nor the cyber security. [...]. A mistake can burn that asset. »*

13. Entretien avec l'amiral Michael Rogers, ancien directeur de la NSA (2014-2018), par appel vidéo, le 3 mars 2023. Citation originale (traduite par l'auteur) : *« The Ukraine partnership starts in 2014, with Crimea, which is a wake up call for the Ukrainians. They understand they have to increase their games. They had a really good attitude. They wanted to listen, to learn.*

Les équipes de chasse (*Hunt Forward*) de la NSA et du Cybercom, dont la mission est de rechercher des menaces informatiques sur les réseaux d'un allié, ont été efficaces. L'amiral Rogers confirme avoir envoyé plusieurs fois des équipes en Ukraine, entre 2014 et 2018, et le général Nakasone a détaillé l'envoi de la mission de novembre 2021 restée 70 jours, avant et pendant l'invasion[14]. Ces équipes de chasse sont invitées par la nation hôte à se rendre dans le pays et à cartographier les systèmes d'information sensibles, pour ensuite réaliser une recherche des modes opératoires et *malwares* de l'adversaire, afin de les partager et les neutraliser, ce qui rend ces missions utiles pour les deux pays. Pourtant, il a fallu négocier âprement car, en 2021, les Ukrainiens n'en voulaient plus, estimant être prêts et maintenant une méfiance à l'égard de la pénétration informatique américaine. De ces retours d'expérience positifs, le DoD et le Cybercom ont développé la notion *« expeditionary cyber warfare »* en décembre 2022, signifiant la nécessité de déployer des capacités cyber hors des États-Unis pour avoir une vision complète de la menace.

Ce discours américain est à relativiser car les acteurs ukrainiens interrogés estiment qu'avant l'invasion de février 2022, les responsables américains n'étaient pas particulièrement déterminés à aider les entreprises cyber ukrainiennes. La plupart des attaques auraient ainsi été traitées de manière autonome ou *via* des relations commerciales avec les entreprises américaines. Les institutions américaines entretenaient un dialogue soutenu avec le SBU, par exemple, qui recevait une formation et de l'équipement de ses partenaires américains, mais ce dialogue relevait plus d'un échange à double sens. Le changement a eu lieu après les cyberattaques russes de janvier 2022, date à partir de laquelle des ateliers ont été mis en place par le FBI, le DoD, les agences de renseignement américaines et des acteurs ukrainiens, notamment privés, pour échanger sur les modes opératoires russes. Sur le plan cyber, l'assistance est devenue systématique, de plus en plus substantielle et de confiance. Les restrictions juridiques qui pesaient sur les grandes entreprises américaines ont été levées[15].

It was a sustained effort. It wasn't 6 months support and then we had other priority so we left. No, it was a sustained effort, a level of cooperation maintained over the last 8 years. […] The Ukrainians are good. They were not starting from zero. They were smart, intelligent and they had abilities. Very good abilities.»

14. Le site du Cybercom évoquait 44 missions dans 22 pays dont l'Albanie, l'Ukraine, l'Estonie, la Lituanie, la Croatie, le Monténégro et la Macédoine du Nord depuis 2018.

15. Entretien anonyme avec un responsable d'une entreprise ukrainienne de cybersécurité, par appel vidéo, le 2 mars 2023.

Hérodote, n° 190-191, La Découverte, 3e et 4e trimestres 2023.

Le rôle central des entreprises américaines depuis 2014

Les entreprises américaines de cybersécurité se sont installées, dès 2013-2014, en Ukraine pour offrir leurs services au gouvernement ukrainien avant même la prise de la Crimée. Au début, ce n'est pas le secteur privé, mais les institutions ukrainiennes qui ont sollicité l'aide de ces entreprises. En effet, l'Ukraine était devenue un hub du cybercrime en 2010, aussi ces entreprises ont-elles fourni des services de sensibilisation aux risques cyber, de formation en cybersécurité et d'identification de la menace cyber : à titre d'exemple, la cyberpolice ukrainienne a été formée par des entreprises américaines[16].

Ces entreprises américaines ont trouvé un réel intérêt à travailler en Ukraine et dans l'espace européen pour leurs activités de Cyber Threat Intelligence (CTI) c'est-à-dire le travail de compréhension et de caractérisation d'une menace informatique (nature des adversaires, de leurs capacités et de leurs modes opératoires ; identification des vulnérabilités de systèmes informatiques face à ces adversaires). La nécessité de comprendre en profondeur les modes opératoires utilisés par les cybercriminels russes et ukrainiens était indispensable pour parfaire les solutions commerciales. Des sociétés comme Microsoft, Google, Palo Alto, Recorded Future, Crowdstrike ou Mandiant, pour ne citer que les plus importantes, ont fourni aux acteurs ukrainiens des services dédiés à des aspects différents de la cybersécurité. Le fait que ces entreprises aient souhaité bénéficier de l'expérience ukrainienne pour développer une connaissance des acteurs russes est un point important pour la protection des clients ukrainiens comme des clients et institutions américains, car la position dominante de ces grandes entreprises dans l'espace numérique a permis de diffuser largement la connaissance et d'augmenter la sécurité collective dans le domaine cyber[17].

Dans le cadre de l'invasion de février 2022, les sociétés américaines de cybersécurité se sont montrées très actives pour aider leurs clients, parfois de manière gratuite. Ces entreprises américaines ont fourni des services de protection aux infrastructures numériques ukrainiennes qui se sont avérés déterminants dans la résilience numérique du gouvernement ukrainien. L'invasion a constitué un point de bascule important. Les entreprises américaines fournissant des services de *cloud* avaient déjà proposé d'héberger les données et services informatiques du gouvernement ukrainien, mais ce dernier avait toujours refusé. Toutefois, en raison de l'invasion russe et grâce à la confiance née de plusieurs années de

16. Entretien anonyme avec deux experts en cybersécurité, en entreprise, Washington, le 17 février 2023.

17. *Ibid*.

coopération, le gouvernement ukrainien a accepté de mettre ses données sur les infrastructures *cloud* d'Amazon Web Service et de Microsoft[18] ou de contracter avec Recorded Future pour la sécurité cyber de ses infrastructures critiques[19]. Ainsi, Google a fourni une assistance substantielle aux acteurs ukrainiens, notamment 50 000 licences gratuites « Google Workspace » pour le gouvernement avec un accès au *cloud* sécurisé de Google ou une mise à disposition des institutions ukrainiennes de la protection Project Shield contre les attaques DDoS. La plupart des grandes entreprises ont fourni ce type d'assistance améliorant leur positionnement dans le cyberespace ukrainien, tout en agrandissant le territoire numérique américain. Les entreprises de télécommunication américaines ont aussi participé, telles Verizon, AT&T ou T-Mobile qui ont fourni des services gratuits ou moins chers pour faciliter la communication vers ou depuis l'Ukraine[20].

Les entreprises américaines ont donc un rôle central pour les institutions américaines, car elles disposent d'une relation de proximité et d'obligations contractuelles à l'égard de la NSA et du Cybercom qui leur imposent de partager les renseignements cyber qu'elles collectent sur des acteurs malveillants[21]. L'Ukraine représente un premier cas de coopération entre tous les acteurs du cyber et la crise à venir à Taïwan constituera sans doute le prochain.

En retour, elles permettent à la NSA et au Cybercom de contourner leur méfiance structurelle à l'égard de leurs homologues pour accroître la sécurité des institutions et secteurs critiques ukrainiens. Les entreprises américaines de cybersécurité disposant de relations de longue date avec le gouvernement ukrainien sont souvent utilisées comme intermédiaires pour informer les acteurs ukrainiens de vulnérabilités observées ou de *malwares* identifiés sur leurs réseaux. La NSA et

18. Sebastian Moss, « Ukraine awards Microsoft and AWS peace prize for cloud services & digital support », *Data Center Dynamics*, 07/07/2022, <https://www.datacenterdynamics.com/en/news/ukraine-awards-microsoft-and-aws-peace-prize-for-cloud-services-digital-support/>, consulté le 14/04/2023.

19. Michael Novinson, « Christopher Ahlberg on Recorded Future's Work to Aid Ukraine », *CIO Inc*, 23/12/2022, <https://www.cio.inc/christopher-ahlberg-on-recorded-futures-work-to-aid-ukraine-a-20797>, consulté le 13/04/2023.

20. Taylor Sanzo, « T-Mobile, AT&T, Verizon among cellphone carriers supporting Ukraine by waving charges, allowing free long-distance calls to the country », *Mass live*, 01/03/2022, <https://www.masslive.com/news/2022/03/t-mobile-att-verizon-among-cellphone-carriers-supporting-ukraine-by-waving-charges-allowing-free-long-distance-calls-to-the-country.html>, consulté le 14/04/2023.

21. Ce partage s'inscrit dans le cadre des échanges sur la menace cyber et ne correspond pas aux requêtes formulées par la NSA vers des entreprises américaines dans le cadre de la collecte classique de renseignement (sous mandat FISA 702). Entretien anonyme avec deux experts en cybersécurité, en entreprise, Washington, le 17 février 2023.

Hérodote, n° 190-191, La Découverte, 3e et 4e trimestres 2023.

le Cybercom effectuent des signalements aux entreprises, ce qui permet à ces dernières de remédier au problème ou de le répercuter à leurs clients ukrainiens sans risquer de compromettre les accès techniques sensibles américains ayant permis ces détections.

Cette relation institutionnelle entre les entreprises de cybersécurité et les institutions américaines est le fruit d'une nécessaire coordination, mais aussi du fait que ces entreprises sont sur le « front cyber » et disposent d'une vision plus étendue et complète que les institutions américaines, notamment en raison des contraintes légales et des difficultés d'accès qui s'imposent à ces dernières. Ce différentiel s'accroît avec l'extension de la surface numérique de ces entreprises, à mesure qu'elles développent leurs relations de clientèle dans le monde.

Une relation de renforcement mutuel et de codépendance

L'autonomie stratégique ukrainienne renforcée par le soutien américain…

L'autonomie stratégique est un concept issu de la culture stratégique française. L'expression apparaît pour la première fois dans le livre blanc de 1994 et se trouve étroitement reliée à la dissuasion nucléaire française. Elle est entendue comme « l'indépendance et la liberté d'action politique », mais se trouve aussi définie par ce qu'elle n'est pas, à savoir « des dépendances contraires au principe de notre autonomie stratégique »[22]. Ainsi, elle relie directement les enjeux de dépendances à l'autonomie. Le concept est défini plus précisément dans le livre blanc de 2008. Il s'agit de garantir « la liberté d'appréciation, la liberté de décision et la liberté d'action du chef de l'État[23] ».

Plusieurs enquêtés ont fait le constat que la défense ukrainienne a tenu avant tout grâce aux Ukrainiens eux-mêmes, dont les capacités ont été sous-estimées par les acteurs américains. Les responsables américains estimaient en effet que le gouvernement et les forces ukrainiennes ne tiendraient pas face aux forces armées russes. En réalité, la transition d'une armée sur le modèle soviétique, en 2014, à une armée formée aux standards OTAN, en 2022, a eu un impact réel sur le terrain, confirmant la nette amélioration de l'efficacité des forces ukrainiennes[24].

S'agissant des domaines cyber et du renseignement, Gavin Wilde et Mike Rogers, tous deux anciens membres de la NSA, estiment que si la NSA et le

22. Livre blanc sur la défense, 1994, p. 50.

23. « Défense et sécurité nationale », livre blanc, 2008, p. 69.

24. Entretien anonyme avec un responsable de la sécurité nationale, Washington, le 14 février 2023.

Cybercom ont apporté une aide substantielle dans la durée, les responsables ukrainiens du domaine cyber avaient largement intégré les leçons et pratiques partagées devenant des acteurs efficaces et autonomes dans le domaine de la cyberdéfense. L'aide reçue autant que l'expérience acquise en étant soumis à des attaques russes leur ont permis de s'améliorer. Dans le cyber, cette autonomie s'illustre de plusieurs manières[25] :

- Les acteurs américains ont dépassé leur méfiance vis-à-vis de leurs homologues ukrainiens et accru le volume de leurs échanges, confirmant en creux la crédibilité et le degré d'autonomie attribués à ces derniers.
- La politique offensive cyber menée avec les cyberpartisans de l'IT Army of Ukraine est un choix ukrainien qui ne correspond pas aux standards américains.
- Le niveau technique des acteurs ukrainiens du cyber est devenu si bon qu'ils exportent désormais leur savoir-faire à l'international, renforçant d'autant l'autonomie du pays en matière cyber et économique.

Le gouvernement ukrainien a utilisé différents leviers de la coopération pour se rapprocher de ses objectifs stratégiques (éloignement de la Russie ; rapprochement avec l'UE et l'OTAN). En me référant aux définitions de l'autonomie stratégique, je considère que ce mouvement fait apparaître de nouvelles dépendances, mais que celles-ci ont été recherchées par le gouvernement ukrainien. La capacité du gouvernement et des forces armées ukrainiennes à résister à la Russie pour garantir au peuple ukrainien le respect de sa souveraineté est un choix politique qui a été effectué par le gouvernement en contradiction avec les évaluations de l'allié américain, confirmant la liberté d'appréciation, de décision et d'action du président Zelensky et de son gouvernement, liberté ainsi renforcée par l'aide américaine.

... mais des dépendances naissantes à l'égard des États-Unis

Les choix stratégiques faits par le gouvernement ukrainien impliquent de concéder de nouvelles dépendances à l'égard des « nouveaux alliés », États-Unis en tête. Elles ne sont pas subies, comme dans le cas des rapports de domination que souhaitait imposer la Russie, mais procèdent de la notion de dépendance au sentier[26], au sens où elles risquent d'insérer le gouvernement ukrainien dans le

25. Entretien anonyme avec un responsable d'une entreprise ukrainienne de cybersécurité, par appel vidéo, le 2 mars 2023.

26. Notion issue de la littérature scientifique relative à l'institutionnalisme et à l'inertie des organisations, qui tend à démontrer qu'une structure politique ou administrative, même soumise à un choc, ne change pas radicalement ses pratiques [Greener, 2005].

Hérodote, n° 190-191, La Découverte, 3e et 4e trimestres 2023.

sillon stratégique américain pour de nombreuses années, et du jeu d'alliances, au sens où ces relations impliquent une espérance de gains en échange de pertes consenties. Le soutien et la formation fournis par les acteurs américains, mais aussi l'engagement militaire, cyber et renseignement à leurs côtés construisent en Ukraine des dépendances dans la durée :

- L'utilisation massive d'armements américains et européens organise une dépendance aux technologies et équipements. De la même manière, dans le domaine cyber, l'extension de la clientèle des entreprises américaines de cybersécurité accroît la dépendance des acteurs gouvernementaux et privés à leurs services informatiques.
- L'invasion russe a renforcé l'opportunité pour la NSA et le Cybercom de se positionner dans les réseaux russes. La confrontation, militaire et politique, entre l'Ukraine et la Russie risque de durer encore plusieurs années et les capacités cyber-américaines resteront vraisemblablement importantes pour la défense de l'Ukraine, créant une dépendance à ces dernières.

Le stockage des données souveraines ukrainiennes dans des *cloud* américains accroît mécaniquement la dépendance ukrainienne à ces services. Dans le cas présent, cette décision peut être vue comme un accroissement de la souveraineté ukrainienne, en particulier de son autonomie stratégique : le gouvernement ukrainien dispose d'un accès protégé et sans entrave à ses données. Cette décision peut aussi être vue comme faisant obstacle au plein exercice de la souveraineté ukrainienne, dès lors que des opérations de renseignement américaines sur ces serveurs américains peuvent fournir une connaissance des actions ukrainiennes non voulue par le gouvernement ukrainien. Ce choix stratégique est intrinsèquement dual, en ce qu'il constitue à la fois une vulnérabilité et une force, en fonction de l'acteur dont souhaite se protéger le gouvernement ukrainien.

La dépendance à des technologies privées américaines accroît la dépendance vis-à-vis d'entités moins prévisibles que le gouvernement américain. Ainsi, en septembre 2022, Elon Musk, PDG de Starlink, a choisi de changer de stratégie et d'exiger publiquement le paiement du service fourni aux autorités ukrainiennes, au risque de l'arrêter. Sur un sujet aussi central alors que la guerre est en cours, ces aléas constituent des obstacles stratégiques.

Il existe un pouvoir politique et de coercition détenu par les acteurs qui disposent d'un pouvoir de réseau construit sur des interdépendances imposées dans les domaines économiques et de l'information [Farell et Newman, 2019]. Les dépendances construites par le partenariat entre l'Ukraine et les États-Unis offrent un pouvoir politique et topologique très fort au gouvernement américain pour servir ses propres objectifs. Ce pouvoir est renforcé par la position centrale de l'acteur, ici les États-Unis, au sein d'un réseau international (de biens, d'argent ;

mais aussi « d'informations et d'énergie » pour citer Gilles Deleuze). Henry Farrell et Abraham Newman écrivent :

> S'ils disposent d'institutions nationales appropriées, ils peuvent « militariser/instrumentaliser » les réseaux pour recueillir des informations ou étouffer les flux économiques et d'informations, découvrir et exploiter les vulnérabilités, imposer un changement de politique et dissuader les actions indésirables. Nous identifions et expliquons la variation de deux stratégies par lesquelles les États peuvent obtenir de puissants avantages en militarisant l'interdépendance ; ils s'appuient respectivement sur un effet « panoptique » et un effet « goulot d'étranglement » des réseaux. Dans le premier cas, les États favorisés utilisent leur position sur le réseau pour extraire des avantages informationnels vis-à-vis des adversaires, alors que, dans le second, ils peuvent couper les adversaires des flux du réseau.

Les États-Unis sont en mesure d'instrumentaliser leurs relations avec le gouvernement ukrainien par les deux effets évoqués : l'effet « panoptique » permis par les renseignements collectés par les États-Unis, notamment dans le domaine cyber, grâce à leur présence en Ukraine ; l'effet « goulot d'étranglement » s'applique dès lors que les flux de renseignement et d'armement partagés avec les acteurs ukrainiens leur sont vitaux. Dans ce cadre, la NSA est un acteur central pour permettre au gouvernement américain d'exploiter ces interdépendances.

Une relation de codépendance : les besoins américains

Plusieurs enquêtés ont souligné l'importance, pour les acteurs américains du cyber, du gain que leur offre leur coopération avec l'Ukraine. La richesse des informations partagées offre une protection supplémentaire au territoire numérique américain, rendue possible à plusieurs reprises par un échange constant sur la menace (code des pièges informatiques, vulnérabilités des systèmes d'information) avec l'écosystème américain et parfois allié. Ce partage quotidien entre les acteurs ukrainiens et américains, mais aussi leurs alliés, leur a offert la possibilité de sécuriser leurs propres réseaux[27]. Cette cyberdéfense devient plus efficace car elle fonctionne en réseau, dans une logique distribuée où de nombreux savoirs et outils sont mutualisés ou partagés par tous les membres de ce réseau. Cette organisation est assez spécifique au domaine cyber et renforce l'intérêt des logiques d'alliance. En ce sens, la défense des réseaux américains, premières cibles des cyberattaques à l'échelle du globe, est particulièrement dépendante des échanges avec les acteurs ukrainiens.

27. Entretien anonyme avec deux experts en cybersécurité, en entreprise, Washington, le 17 février 2023.

Hérodote, n° 190-191, La Découverte, 3e et 4e trimestres 2023.

La notion de dépendance au sentier fonctionne donc dans les deux sens. Les engagements pris par les acteurs américains auprès des acteurs ukrainiens sont par nature moins engageants structurellement. Néanmoins, sur le plan politique, ils limitent la manœuvre stratégique des États-Unis à l'avenir car, en s'engageant auprès du gouvernement ukrainien, pour éloigner durablement la menace russe de son territoire numérique, Washington éloigne également toute future tentative de rapprochement ou de *reset* avec Moscou.

Conclusion

Cette extension du territoire numérique des États-Unis est rendue possible à la fois par une combinaison d'actions autonomes des entreprises, de stratégies diversifiées et parfois rivales des acteurs institutionnels et de stratégies volontaires des acteurs ukrainiens, et par la difficulté des acteurs concurrents, notamment européens, à formuler eux-mêmes des politiques adaptées. Le gouvernement américain n'est pas le chef d'orchestre omnipotent d'une politique de puissance américaine ; celle-ci est facilitée par une conjonction de facteurs qui dépassent la seule volonté stratégique des responsables politiques américains.

En revanche, l'exploitation de ces opportunités permise par les réflexes nés d'un cadre culturel et stratégique partagé par l'ensemble de l'écosystème cyber et du renseignement, mais aussi le cadre politique et réglementaire permissif américain sont à l'origine d'un système performant de surveillance et de protection du territoire numérique américain, dont le partenariat avec l'Ukraine est devenu un atout considérable. Taïwan offrira-t-il le même levier ?

Bibliographie

BALTHAZAR L. (2022), « Chapitre 3. Le cadre culturel. Le style national » dans DAVID C.-P. et TOURREILLE J. (dir.) (2022), *La Politique étrangère des États-Unis*, 4e édition, Paris, Presse de Sciences Po, p. 99-p131.

CATTARUZZA A. et LIMONIER K., *Introduction à la géopolitique*, Paris, Armand Colin, 2019.

FARELL H. et NEWMAN A. (2019), « Weaponized Interdependence: How Global Economic Networks Shape State Coercion » dans « The President and Fellows of Harvard College and the MIT », *International Security*, vol. 44:1, 2019, p. 42-p. 79.

GREENER I. (2005), « The Potential of Path Dependence in Political Studies » dans *Politics*, vol. 25:1, Blackwell Publishing Ltd, 2005, p. 62-p. 72.

LACOSTE Y. (dir.) (1993), *Dictionnaire de géopolitique*, Paris, Flammarion.

PETINIAUD L. (2014), « Cartographie de l'affaire Snowden » dans DOUZET F. (dir.) (2014), *Cyberespace : enjeux géopolitiques*, Paris, Éditions La Découverte, p. 35-p42.