note n°02/2014

23 janvier 2014

FONDATION pour la RECHERCHE STRATÉGIQUE

**Vincent Joubert**
Chargé d'étude, Fondation pour la recherche stratégique
**Gergana Petkova**
Fondation pour la recherche stratégique

# L'intégration des citoyens dans une stratégie nationale de cyberdéfense

## Entre opportunités et contraintes stratégiques

*Résumé*

Avec 2,7 milliards d'internautes dans le monde en 2013, une accessibilité facilitée par la multiplication de technologies d'accès à Internet et des prix décroissants, il n'est plus possible aujourd'hui pour les États d'ignorer les conséquences potentielles d'actions entreprises par des citoyens agissant seuls ou en groupes dans le cyberespace. Alors que la majorité des États a mis en place une stratégie nationale de cybersécurité et de cyberdéfense, la relation entre gouvernements et citoyens internautes n'est que peu abordée dans la littérature actuelle. Cette note propose ainsi une analyse succincte des opportunités et limites de l'intégration des citoyens dans une stratégie nationale de cyberdéfense.

*Abstract*

*With 2.7 billion Internet users in 2013, and greater network accessibility made possible by more affordable mobile technology devices, nation states can no longer ignore the potential impact of individuals' actions in cyberspace. Isolated skilled hackers or cybermilitias can play an important role in cyberconflicts, which governments have to anticipate in order to prevent unexpected events. This short paper analyzes the relations between organized civilian groups of hackers and governments in cybersecurity activities, and outlines the strategic consequences of integrating civilian hackers in a cyberoperation.*

Les caractéristiques du cyberspace affectent directement la pratique de la politique au niveau international et national : l'instantanéité remplace la temporalité conventionnelle des espaces physiques, la notion de géographie est érodée, la perméabilité des frontières et des juridictions traditionnelles est inévitable, l'instabilité, entendue ici comme la reconfiguration permanente des différentes couches du cyberspace due aux évolutions technologiques, est, elle aussi, inéluctable, la participation à l'activité politique est facilitée par la disparition des barrières traditionnelles relatives à l'expression publique, l'identification ou l'attribution des actions est techniquement très compliquée et permet d'agir dans un certain anonymat, et enfin les mécanismes juridiques classiques permettant d'engager la responsabilité d'un acteur sont contournés. Par conséquent, le cyberespace offre aux individus de nouveaux moyens d'expression et d'action politique sans précédent. Cette valorisation de leur participation dans la politique publique se manifeste par des prises de positions, la communication de leurs opinions, et éventuellement l'organisation d'actions (individuelles ou collectives) dont le but est de défendre une ligne politique ou idéologique, soutenant ou s'opposant à une action menée par les autorités politiques d'un État[1].

Ainsi, l'État n'a pas le monopole de l'action dans le cyberespace, fût-elle défensive ou offensive. En effet, le cyberespace est composé d'un ensemble hétéroclite d'acteurs étatiques et non-étatiques, publics et privés, avec des intérêts, des attentes, des capacités, et des objectifs propres à chacun. Avec aujourd'hui 2,7 milliards d'internautes dans le monde, il n'est plus possible pour les États d'ignorer l'impact potentiel que peut avoir une action menée individuellement ou collectivement par des internautes civils (i.e non-militaires, n'agissant pas sur ordre ni pour le compte de l'État).

Certains États ont parfaitement pris la mesure du vivier que représentent les internautes civils et ont décidé de les impliquer, officiellement ou officieusement, dans des activités offensives et défensives servant les intérêts de l'État, avec plus ou moins de succès, mais révélant cependant une certaine tendance qu'il convient d'analyser pour mieux l'appréhender.

1. Nazli Choucri, *Cyberpolitics in International Relations*, The MIT Press, Cambridge, Mass., 2012.

## Le patriotisme comme principal moteur de mobilisation

Les exemples d'implication d'internautes civils dans des conflits inter-étatiques ou lors d'événements liés à des tensions diplomatiques ne manquent pas : des attaques en *distributed denial of services* (DDoS) contre le site internet de l'OTAN lors des campagnes dans les Balkans dans les années 1990, des attaques DDoS contre les réseaux militaires des États-Unis suite au bombardement de l'ambassade de Chine en Yougoslavie, ou encore en 2001 suite à l'affaire de l'avion espion à Hainan[2]. En 2007, des attaques répétées contre les systèmes d'information (SI) et réseaux de l'Estonie ont pu bénéficier d'une organisation orchestrée via des forums et sites russes dans lesquels des instructions étaient fournies pour mener les attaques. L'année suivante, des attaques DDoS inondent les sites internet du gouvernement et des principaux médias géorgiens au moment où les troupes russes pénétraient sur le territoire ; un forum de hackers russe spécialement mis en place revendiquait même ouvertement être à l'origine des opérations[3].

Depuis environ 5 ans, le recours à des attaques DDoS politiquement motivées se sont multipliées, qu'elles soient le résultat d'une action visant à « punir » un comportement ou une action d'un adversaire politique, ou qu'elles visent à empêcher toute diffusion d'information véhiculant des positions allant contre le régime politique en place. Dans la majorité des cas, les attaques lancées par des internautes civils font appel à un sentiment de patriotisme voire de nationalisme, soutenant la position de leur gouvernement contre des opposants internes ou externes. L'utilisation de cyberattaques de faible intensité et peu sophistiquées (comme c'est le cas des DDoS) peut alors s'apparenter à une tactique de guérilla numérique par laquelle les internautes civils manifestent ce soutien idéologique et patriotique[4]. D'autre part, l'exposition médiatique de leurs actions permet également une diffusion publique plus large de leurs positions politiques et facilite de fait la propagande qui accompagne systématiquement ce genre d'action. Cependant, la diffusion médiatique des revendications patriotiques ou natio-

2. Jose Nazario, « Politically Motivated Denial of Service Attacks », in Czosseck, C. & Geers, K. (Eds.) *The Virtual Battlefield: Perspectives on Cyber Warfare. Proceedings 2009*. Amsterdam: IOS Press.

3. *Ibidem.*

4. Ibid.

nalistes peut également déclencher un mouvement de réponse, elle-même motivée par un sentiment patriotique, des adversaires ou opposants politiques-idéologiques du premier.

La récupération patriotique de tensions internationales dans le cyberespace est remarquablement commune. Elle n'est pas limitée à une région géographique, ni à un type de régime politique, ni même à la cause des tensions ou des conflits. Elle n'est pas non plus propre à un type d'acteur : les individus peuvent spontanément décider de mener des représailles mues par leurs sentiments patriotiques, mais les États peuvent stimuler ce sentiment pour servir des intérêts stratégiques de leur politique extérieure. Le soutien de l'État pour ce genre d'actions peut être actif (comme ce fut le cas pour les attaques en Estonie[5]) mais également passif, par lequel l'autorité politique au pouvoir ne procède à aucune poursuite judiciaire contre des individus ayant lancé des attaques depuis son territoire ; cette protection tacite est perçue depuis l'extérieur comme un soutien gouvernemental indirect. Cette forme de soutien bénéficie d'ailleurs des limites actuelles considérables de l'encadrement juridique des collaborations en termes de procédures judiciaires internationales[6].

Étant donné l'augmentation quantitative des citoyens connectés, et l'augmentation qualitative des services d'accès à Internet dans toutes les régions du globe[7], il y a toutes les raisons de penser que l'implication d'internautes civils dans les conflits actuels et futurs soit amenée à s'accroître. La récupération idéologique et politique de conflits amènera inévitablement des groupes d'internautes à agir dans le cyberespace pour défendre leurs causes, leurs valeurs, leurs idéologies. La formation de ces groupes, appelés les *cyber-milices*, et leur implication dans les conflits peut entraîner des complications dans leur résolution diplomatique, dans la mise en œuvre opérationnelle de la stratégie développée par un des protagonistes, et pourrait dans le pire des cas entraîner une escalade dans le conflit. Cet aléa stratégique contraint les États à prendre en compte les activités de ces cyber-milices afin d'anticiper au maximum leurs réactions et ne pas mettre en péril leurs intérêts.

On constate à l'heure actuelle deux politiques distinctes par lesquelles les gouvernements intègrent ces citoyens dans leurs capacités de cyberdéfense, et qu'il convient de distinguer.

D'un côté, un certain nombre d'États ont lancé des programmes permettant de cibler et réunir les citoyens qui, par leur expertise et leur patriotisme, constitueront une réserve citoyenne volontaire qui pourra être sollicitée en cas d'attaques sur les SI de la nation. C'est le cas en France, avec la *Réserve Cyber Citoyenne*, en Estonie avec la *Estonian Defense League's Cyber Unit*, ou le Royaume-Uni avec la *Joint Cyber Reserve*. Le champ d'action de ces réserves citoyennes est strictement encadré juridiquement, et tout acte dépassant les prérogatives accordées devient dès lors illégal et engagera la responsabilité individuelle de son auteur. Aux États-Unis, la situation est légèrement différente ; si le US Cyber Command dispose de moyens humains, technologiques et financiers sans pareil pour assurer la protection des intérêts américains dans le cyberespace, l'incapacité du gouvernement actuel à légiférer pour imposer des standards techniques et procéduriers de sécurité au secteur privé – qui détient la grande majorité des infrastructures critiques du pays – force la communauté d'experts à envisager la création d'une réserve citoyenne, soit sous une forme similaire à la Garde nationale[8], soit sur la base du système « *Neighborhood Watch Program* », dans lequel les citoyens seraient appelés à surveiller toute activité malveillante sur les réseaux[9]. Dans tous les cas, ces réserves citoyennes cyber agissent en conseillers techniques, et non comme des forces des opérations spéciales. Leurs prérogatives étant clairement définies et encadrées, les réserves citoyennes ne posent pas de problèmes.

D'un autre côté, des États ont recours aux internautes citoyens organisés en groupes aux intérêts communs, les *cyber-milices*, n'hésitant pas à les impliquer concrètement dans leurs opérations dans le cyberespace (dans une certaine mesure). Les autorités gouvernementales jouent sur les mêmes leviers, patriotisme et sens du devoir envers la nation, pour recruter les citoyens disposant de connaissances suffisantes en informatique. Il est d'ail-

5. *Ibid.*, voir notamment le rôle des « Russians Youth Groups » et leurs relations ambigües avec le Kremlin.

6. Maeve Dion, « Different Legal Constructs for State Responsibility », in *International Cyber Security Legal & Policy Proceedings*, Eneken Tikk & Anna-Maria Talihärm (Eds.), CCD COE Publications, 2010, pp. 67-75.

7. International Telecommunication Union, *Measuring the Information Society 2013*, ITU Report, 2013.

8. http://www.nextgov.com/cybersecurity/2012/10/dhs-urged-create-reserve-cadre-cyber-experts/58704/

9. Jake Mihevc, « *The Formation of Cyber Militias in the United States : Feasibility, Structure and Purpose* », *http://blogs.csoonline.com/global-security/2306/formation-cyber-militias-united-states-feasibility-structure-and-purpose-jake-mihevc*

leurs intéressant de constater que dans ces pays où le sentiment de patriotisme est extrêmement présent, des cyber-milices se sont formées spontanément pour combattre « les ennemis de la nation » dans le cyberespace. D'autres groupes de hackers, dont l'activité première n'est pas de mener des attaques politiquement motivées mais plutôt la cybercriminalité (très lucrative), n'en viennent pas moins à prêter main forte lorsque les circonstances le demandent et quand ils y trouvent un intérêt. Ainsi, en Russie comme en Chine, les autorités gouvernementales n'ont pas officiellement créé de réserves citoyennes mais des milices civiles existent et sont parfaitement identifiées, et l'aide à la protection et à la défense du cyberespace est considérée comme un devoir citoyen par Moscou et Pékin. En Russie, bien que le piratage informatique contre des SI externes soit officiellement interdit, il est officieusement toléré tant que les hackers ne s'en prennent pas aux intérêts ou aux infrastructures de l'État. Cet accord tacite permet aux hackers menant des activités de cyber-criminalité de ne pas être inquiétés par la justice nationale et offre au Kremlin une force complémentaire dotée d'une véritable expertise technique informatique[10]. En Chine, les relations entre les unités de l'Armée Populaire de Libération (PLA) et un bon nombre d'internautes civils dans leurs activités dans le cyberespace sont assez floues, le gouvernement incitant les citoyens à participer activement à la « surveillance » des réseaux afin de garantir la sécurité de tous et de la Chine. Cette participation a une double finalité : d'une part prévenir toutes dissidences au régime sur le plan national (par de la dénonciation et de la censure), et aider la PLA dans ses activités externes dans le cyberespace.

## Les bénéfices et les limites de l'implication de cyber-milices dans une stratégie de cyberdéfense

Impliquer des internautes dans les actions de cyberdéfense de l'État soulève cependant énormément d'interrogations quant à la collaboration en pratique, l'intérêt stratégique, ou encore la légalité et la responsabilité opposable face à de telles actions.

La collaboration avec des cyber-milices de citoyens volontaires nécessite quelques prérequis inhérents à l'organisation même des cyber-milices, mais également des rôles et responsabilités qui leur seront attribués. Les cyber-milices sont un regroupement d'internautes partageant et voulant défendre des mêmes idées ; cependant, tous les membres au sein d'un même groupe n'ont pas un même niveau d'expertise et ne pourront donc pas prétendre à effectuer des tâches identiques. De plus, l'existence d'une hiérarchie au sein des cyber-milices n'est pas toujours avérée. Les organisations internes varient énormément d'un groupe à l'autre. R. Ottis identifie ainsi trois types d'organisation : le *forum*, la *cellule*, la *hiérarchie*[11].

- Le *forum* est une plateforme en ligne où les membres peuvent discuter, organiser et distribuer des instructions, des outils, pour effectuer une cyberattaque. Les compétences varient au sein de ce type d'organisation, mais le *forum* présente de nombreux avantages : mobilisation rapide, anonymat, répartition des tâches en fonction des compétences, versatilité. Toutefois, il est très difficile de contrôler les activités des membres, la coordination n'est pas toujours optimale, le manque de compétence est pénalisant, et la liberté d'accès à ces forums pose un risque d'infiltration par les autorités qui pousse les membres impliqués dans des activités criminelles à ne pas privilégier ce type d'organisation[12].
- La *cellule* regroupe des membres qui se connaissent et dont la collaboration est basée sur la confiance. Les membres d'une cellule sont généralement plus expérimentés que ceux d'un forum, et sont souvent impliqués dans des activités de cybercriminalité. La *cellule* ne dispose pas d'un type de gestion propre, on peut trouver des cellules avec des organisations hiérarchiques, ou avoir une simple coordination des activités des membres. La mobilisation d'une cellule est très rapide, et la connaissance réciproque des membres en fait une organisation assez imperméable aux infiltrations des autorités. Cependant, la *cellule* possède des faiblesses non négligeables ; avec la sophistication des actions apparaissent plusieurs éléments susceptibles de déstabiliser ce type d'organisation. Des attaques sophistiquées impliquent généra-

10. Kellermann T., "Peter the Great Vs. Sun Tzu", Trend Micro Inc., Opinion Piece, September 2012.

11. Rain Ottis, *A Systematic Approach to Offensive Volunteer Cyber Militia*, Thesis on Informatics and System Engineering, TUT Press, 2011.

12. Ibid.

lement une spécialisation du hacker, avec un *modus operandi* propre, qui peut révéler son identité, et détruire la notion de confiance au sein du groupe. De même, la sophistication des attaques engendre une hiérarchie informelle basée sur la reconnaissance par les pairs de la complexité de l'exploit technique réussi par le hacker. Or une telle hiérarchie met en jeu des égos et la fierté des personnes qui peuvent être manipulées pour créer une discorde au sein de la cellule. Néanmoins, force est de constater que peu de hackers ayant une expertise de haut niveau manifestent des velléités politiques concrétisées par des actions offensives dans le cyberespace. Dans ces conditions, le niveau d'expertise des membres d'une cellule se traduit majoritairement par des attaques moyennement sophistiquées dont les conséquences ne sont au final pas très importantes[13].

- Enfin, la *hiérarchie*, comme son nom l'indique, correspond à une organisation traditionnelle pyramidale où chacun a un rôle et des responsabilités prédéfinis, avec une chaîne opérationnelle identifiable. Ce type de structure est, pour Ottis, « *l'option la plus probable pour une entité soutenue par un État, en ce qu'elle offre une structure formelle et compréhensible disposant en plus d'une chaîne opérationnelle établie* »[14]. Ainsi, la *hiérarchie* permet d'avoir une force d'action organisée, disposant d'une capacité de commandement et de contrôle interne, établie dans le temps (contrairement aux autres formes d'organisation qui se créent *ad hoc* et agissent *a posteriori*), au sein de laquelle il est possible de prévoir des entraînements, voire de la reconnaissance. Cependant, comme toute organisation structurée, les membres cruciaux (les chefs) deviennent des cibles privilégiées, et intégrer une *hiérarchie* impose d'avoir un niveau d'expertise élevée doublé d'une volonté de devoir répondre à un supérieur hiérarchique[15].

Les trois modèles d'organisation de cyber-milice décrits par R. Ottis permettent de nous rendre compte de la complexité d'une éventuelle collaboration État – cyber-milice. En effet, la plupart de ces structures *réagissent* à des événements d'actualités ; les milices se constituent *ad hoc* pour des actions ponctuelles de faible sophistication, comme des attaques en DDoS ou des défigurations de sites web (*web pages defacement*) qui dépassent peu souvent le stade de nuisance[16]. Les cas d'études où une organisation d'internautes civils volontaires a été sollicitée par un État (Géorgie, Estonie) nous apprennent que les « tâches confiées » restent de basse intensité technique, ce qui n'enlève rien à leur visibilité et à leur effet de nuisance. Les États ne se tourneront pas vers des civils dont ils ignorent tout pour mener des opérations plus sophistiquées.

Dès lors, quel intérêt stratégique un État peut-il trouver dans l'implication d'internautes civils pour mener des opérations défensives ou offensives dans le cyberespace ? Les opérations de nuisance confiées aux cyber-milices n'affectent habituellement pas les intérêts de la nation mais ont un écho médiatique et donc public important. Cet écho peut avoir des conséquences duales : il peut dissuader un adversaire de persévérer dans la conduite de son action qui est à l'origine des cyber-attaques (par crainte de voir le conflit s'aggraver), comme il peut au contraire entraîner cette escalade dans le conflit (et pousser l'adversaire à lancer des représailles). D'autre part, cet écho médiatique peut, dans ces cas d'attaques nombreuses et ciblant des sites web grand public, générer une pression de l'opinion publique exhortant les décideurs politiques à agir plus rapidement ou plus fermement contre les attaquants. Or, précipiter une réaction contre des cyber-attaques de nuisance n'a pas d'intérêt stratégique avéré pour l'État et risque au contraire d'envenimer la situation[17]. Dans ces conditions, on peut envisager un compromis dans lequel les cyber-milices seraient sollicitées pour mener des actions contre les cyber-milices adverses, et dont l'objectif serait d'empêcher les adversaires de mener à bien des attaques de nuisances. Les actions des cyber-milices ciblant ainsi celles de leurs pairs, elles limiteraient les attaques visibles par le grand public (la défiguration de sites web notamment) et permettraient aux services de l'État de se focaliser sur la poursuite des opérations.

13. *Ibid.*

14. *Ibid.*

15. *Ibid.*

16. Il faut bien évidemment garder le sens des proportions. Des attaques en DDoS sur des SI ciblés peuvent considérablement nuire à l'activité d'une entreprise, d'une OIV, ou d'une institution étatique.

17. Voir les travaux de M. Libicki sur les représailles dans le cyberespace : *Cyberdeterrence and Cyber War*, RAND Copr, 2009 ; et *Crisis and Escalation in Cyberspace*, RAND Corp., 2012.

Ainsi, en maintenant une action à un niveau qui correspond à leurs compétences techniques, et une participation dont l'impact stratégique et politique est limité, les cyber-milices pourraient jouer un rôle non-négligeable tout en affectant le moins possible la stratégie de l'État et le déroulement des opérations.

L'intérêt stratégique réel lié à l'implication de cyber-milices résiderait alors dans l'immunité juridique qu'elle permet actuellement. En effet, depuis que le cyberespace est au cœur des priorités de sécurité pour les États, le problème de l'attribution des attaques inhibe la mise en place d'outils de répression juridique internationaux. L'impossibilité d'identifier formellement l'attaquant empêche toutes actions visant à engager sa responsabilité juridique et permet ainsi aux acteurs du cyberespace de continuer à opérer sans risquer de sanctions juridiques internationales. Dès lors, un État pourra envisager de déléguer certaines actions dans le cyberespace à des cyber-milices sans voir sa responsabilité engagée *a posteriori*, et quand bien même la cyber-milice serait identifiée, l'État pourra toujours nier tous liens avec celle-ci. Le flou juridique actuel bénéficie à l'État, qui en l'absence de cadre juridique international contraignant, a toute autorité pour prendre les mesures qui lui sembleront appropriées contre des cyber-milices agissant depuis son territoire. Dans la plupart des cas, le piratage informatique contre des infrastructures est illégal, mais les milices sont tolérées tant qu'elles n'affectent pas les intérêts de l'État. Pour autant, des solutions juridiques sont envisagées pour tenter de combler ce vide et engager la responsabilité des États à des degrés variables selon la situation. Plusieurs travaux proposent ainsi des échelles de responsabilité de l'État dans le cas où une tierce partie utiliserait des serveurs et réseaux situés sur son territoire pour mener une attaque[18], là où d'autres préfèrent s'appuyer sur l'application du droit international humanitaire et le droit des conflits armés pour régler la question[19]. Malheureusement, aucune solution n'a été à ce jour acceptée par la communauté internationale, ce qui laisse libre cours à l'implication d'acteurs non-étatiques pour mener des opérations dans le cyberespace.

18. Voir notamment Jason Healey, « *Beyond Attribution: Seeking National Responsibility for Cyber Attacks* », Atlantic Council Issue Brief, 2011.

19. Le *Tallinn Manual on the International Law Applicable to Cyber Warfare* du CCD CoE est le document le plus souvent cité concernant cette approche.

## Aller chercher les compétences là où elles se trouvent

L'implication de cyber-milices dans l'action de l'État dans le cyberespace ne constitue pas en soi une révolution stratégique ; on se situe dans une certaine continuité qui place les compétences techniques des hackers au centre de la découverte de failles de sécurité ou de vulnérabilités dans les SI et réseaux de l'État, et donc de l'amélioration de leur sécurité, avec toutefois un changement notable des mentalités, où la suspicion vis-à-vis des hackers laisse place à la reconnaissance de leur expertise.

Avec l'avènement du cyberespace comme domaine stratégique prioritaire et le développement exponentiel de services associés à son utilisation, les experts en sécurité informatique se sont retrouvés face à une explosion de demandes d'embauches[20]. La croissance pharaonique de ce secteur d'activité a permis aux multinationales de générer des profits en conséquence, et ainsi d'offrir aux hackers des conditions de travail et des rémunérations que le secteur public ne peut absolument pas contrer. Dans certains cas, les hackers choisissent de se tourner vers des activités criminelles qui génèrent elles aussi un profit colossal par rapport aux compétences qu'elles requièrent[21]. Dès lors, il n'est pas étonnant de constater un déséquilibre dans les effectifs de spécialistes en sécurité informatique entre le secteur privé et le secteur public[22].

Dans ces conditions, il n'est pas non plus étonnant de constater que les autorités publiques chargées de la cybersécurité ont régulièrement recours à des entreprises du secteur privé pour venir en aide à un opérateur d'importance vitale victime d'une attaque informatique. Si ces institutions publiques représentent l'autorité nationale en matière de sécurité et de défense des systèmes d'information de l'État dont elles dépendent, elles ne peuvent pas systématiquement rivaliser avec le secteur privé en termes de moyens financiers, technologiques, et humains. L'externalisation des services et prestations de cybersécurité se pose ainsi comme

20. Les offres d'emploi s'apparentent plus à des demandes de la part de l'employeur puisque les entreprises dans le secteur d'activités des technologies de l'information et de la communication démarchent les meilleurs hackers à coups de surenchères pour s'assurer leurs services.

21. Voir *Les marchés noirs de la cybercriminalité*, CEIS, étude stratégique, Technologies de l'information, juin 2011.

22. Ce constat est valable même dans les pays où le patriotisme est très prégnant, comme aux États-Unis, ou en Russie.

une solution au déficit de moyens humains et financiers dont les services des États peuvent souffrir.

L'externalisation de la cybersécurité peut également prendre d'autres formes ; certaines entreprises sont ainsi spécialisées dans la vente de failles de sécurité découvertes par leurs équipes de hackers. Proposées à prix d'or, ces failles permettent à leurs acquéreurs de se prémunir de leur utilisation contre leurs propres systèmes tout en offrant un avantage stratégique puisqu'elles pourront éventuellement être utilisées contre un adversaire. Malgré un coût d'achat conséquent, les États sont des clients réguliers et demandeurs, ce qui laisse à penser que ce commerce offre des avantages stratégiques réels pour les acheteurs[23].

Enfin, à l'inverse des prestations de cybersécurité, la recrudescence des offres de prestations de cyberattaques par des groupes criminels organisés soulève de sérieuses interrogations. En effet, si pour le moment ces offres de « *crime as a service* » (CaaS) ou « *hack as a service* » (HaaS) semblent se cantonner à des activités dont le but recherché est le gain financier, la diffusion des analyses de techniques d'attaques informatiques très sophistiquées, comme ce fut le cas après Stuxnet par exemple, permet aux groupes criminels d'apprendre de nouvelles techniques et de potentiellement diversifier leurs services en proposant des prestations ciblant des infrastructures d'importance vitale pour un État. Bien que ce genre d'attaques soit infiniment plus complexe, long, et coûteux à mettre en place, il n'est pas inconcevable d'envisager dans un futur proche des groupes organisés qui proposeraient leurs compétences à des groupes terroristes pour frapper les intérêts d'un État par des cyberattaques.

L'État dans la conduite de ses prérogatives régaliennes s'est tardivement impliqué dans le cyberespace et a ainsi dû rattraper son retard en matière de moyens technologiques et humains en faisant appel aux experts du secteur privé qui, eux, ont profité des opportunités économiques offertes par ce secteur pour développer très tôt leurs activités et leur expertise. De plus, la niche stratégique que représente l'exploitation du cyberespace pour diffuser, amplifier, et projeter sa puissance sur la scène internationale a créé un besoin immédiat de réponse étatique qui s'est traduit par la mise en place de politiques publiques, et l'élaboration de stratégies nationales dédiées au sein de la communauté internationale. A l'instar de la professionnalisation des armées, il est aujourd'hui plus intéressant à court terme pour un État de faire appel à des experts extérieurs par le biais de partenariats public-privé pour pallier les déficits existants et répondre aux besoins immédiats ; néanmoins, sur le long terme, des solutions de formation et de recrutement d'experts en cybersécurité au sein des services de la défense devront être mises en place pour ne pas dépendre du secteur privé. En ce sens, l'externalisation des prestations de cybersécurité s'inscrit dans une logique contextuelle, mais n'est pas irréversible ni définitive. S'il est vrai que la vitesse d'évolution du domaine exige une réactivité et une adaptabilité face auxquelles le secteur privé semble *a priori* plus à même de répondre, les États devront mettre en place des solutions idoines, tant le cyber devient de plus en plus prégnant dans l'exercice de la sécurité et de la défense.

## Conclusion

L'État n'a pas le monopole de la violence dans le cyberespace. Des individus, regroupés en cyber-milices, rompus aux techniques de sécurité informatique et suffisamment déterminés, peuvent mener des actions d'intensité variable, aux conséquences diverses (de la simple nuisance à une vraie atteinte à la crédibilité stratégique de l'adversaire), afin de défendre une idéologie, une opinion ou l'action de son gouvernement. La portée de leur action dépendra de leurs compétences techniques, mais également de leurs cibles. Si le vide juridique actuel permet aux États d'utiliser ce vivier pour désengager leur responsabilité vis-à-vis des actions menées par ces cyber-milices, l'intérêt stratégique réel que représente l'implication de tels groupes dans des opérations militaires est encore faible. Cependant, il se dégage un attrait des États pour utiliser ces groupes de citoyens à des fins de surveillance, où ils agiraient comme des vigiles sur certains réseaux, à même de donner l'alerte en cas d'attaque.

Ainsi, les États ont bien compris que les individus jouent un rôle essentiel dans le cyberespace, et que multiplier les collaborations, formelles ou informelles, contractuelles ou officieuses, permet de mettre à profit leurs compétences et de leur expertise technique au profit des intérêts de la nation. Le défi, à long terme, est de réussir à mettre en place des po-

23. N. Perlroth & D. Sanger, « Nations Buying as Hackers Sell Flaws in Computer Code », *The New York Times*, 13 juillet 2013.

litiques publiques permettant de former et recruter les futurs experts en sécurité informatique au service de l'État. Les différents rapports et stratégies officiels étatiques disponibles vont tous dans ce sens[24], mais la définition du besoin et l'identification des structures de formation éligibles à de tels partenariats requièrent un travail long et rigoureux, ce qui explique les délais de mise en place de ces procédures de formation et de recrutement.◊

24. On peut citer à cet égard les recommandations énoncées dans le rapport du sénateur Bockel n° 681 « La cyberdéfense : un enjeu mondial, une priorité nationale », *www.senat.fr/rap/r11-681/r11-681_mono.html*


## *Auteurs*

Vincent Joubert, chargé d'étude cybersécurité/ cyberdéfense, Fondation pour la recherche stratégique

vjoubert@frstrategie.org

Gergana Petkova a été assistante de recherche, Fondation pour la recherche stratégique