LE RUBICON

Appréhender l'hacktivisme pro-ukrainien face à l'invasion russe

Benjamin Pajot | 30 août 2022

Alors que les bombardements incessants dans le Donbass nous rappellent que la guerre se déploie d'abord dans le champ cinétique avec une cruelle violence, la dimension cyber du conflit ne doit pas pour autant en être oubliée. Si la « cyberguerre » annoncée n'a logiquement pas eu lieu, un phénomène d'ampleur mérite néanmoins d'être appréhendé en propre. Le conflit a ainsi vu la mobilisation de nombreux groupes d'hacktivistes ayant fait le choix de mettre leurs compétences informatiques au service d'un camp ou de l'autre. Contraction des termes *hacker* et activisme, l'hacktivisme désigne communément des pratiques militantes propres au cyberespace ayant recours à des outils numériques d'intrusion et de piratage à des fins d'expression politique. Présents des deux côtés, les hacktivistes diffèrent cependant dans leur structuration (plus ou moins poussée), leur affiliation (plus ou moins proche de services étatiques) et leurs objectifs (plus ou moins politiques). Si l'activité des groupes pro-russes est relativement bien documentée en raison d'une plus longue présence dans le cyberespace et de capacités de nuisance ayant fait leurs preuves, celle des groupes pro-ukrainiens, en dehors de quelques travaux exploratoires mais essentiels, l'est moins. Cela tient probablement au fait que l'engagement des hacktivistes pro-ukrainiens répond à l'invasion, et est de ce fait aussi massif qu'inédit. A l'origine de nombreuses attaques cyber contre les systèmes d'information russes, ceux-ci constituent aujourd'hui des acteurs directs de l'affrontement en cours, en partie négligés, ce pour quoi ils feront l'objet d'une attention privilégiée ici. Car leur structuration et l'étendue de leurs actions soulèvent de nombreuses questions, à la fois en termes d'efficacité, de risques induits et de légalité, dont les États tardent pourtant à se saisir. Dans la mesure où l'hacktivisme en temps de guerre pourrait perdurer au-delà du contexte ukrainien, il apparaît nécessaire d'en mieux saisir les contours dès à présent.

Un élan de mobilisation majeur

Après avoir reculé pendant une dizaine d'années sous l'effet de la répression accrue et de la démobilisation émotionnelle en l'absence de conflit majeur impliquant l'Occident, il semble que l'hacktivisme en temps de conflit effectue son retour avec l'invasion de l'Ukraine par la Russie. Après avoir connu son apogée en 2011 (le collectif Anonymous ayant notamment été très actif lors des « printemps arabes »), il a ensuite chuté fortement depuis 2015, alors que l'attention publique mondiale se détournait progressivement de la Syrie, de l'Irak, et des agissements de l'État islamique. Cette forme particulière de mobilisation collective étant étroitement liée aux enjeux géopolitiques et de droit international, on peut supposer que c'est le double caractère illégal et illégitime de l'agression russe qui a provoqué la réactivation de ce mode d'action, de manière à la fois spontanée et suscitée.

L'activité d'une centaine de groupes de part et d'autre serait ainsi attestée depuis le début de l'offensive russe, ce qui témoigne du prolongement direct du conflit dans le cyberespace. Leur mobilisation est plus ou moins spontanée, étant aussi bien le fait d'individus souhaitant apporter leur contribution, de groupes autonomes plus organisés et rompus à ces pratiques, que d'entités coordonnées par des autorités étatiques.

« Côté russe », il est probable que la majorité des acteurs soit en réalité issue de groupes cybercriminels (Killnet, Conti, RaHDIt/Nemesis, XakNet, Armageddon, Ghostwriter, Turla…) et/ou étatiques (Sandworm, Fancy Bear, Cozy Bear) déjà actifs, mais ciblant avec davantage d'ardeur les intérêts ukrainiens et ceux de leurs soutiens. Ils se livrent aussi bien à des cyberattaques qu'à des opérations informationnelles, voire à une combinaison des deux. Leurs principaux objectifs sont de répandre les multiples récits russes à l'international, de collecter des renseignements et de lancer des représailles contre les États jugés hostiles (la Roumanie, l'Italie, la Lituanie ou la Norvège ont ainsi pu en faire les frais). Si le Kremlin – par le biais de ses services de renseignement notamment – a pour habitude d'externaliser une partie de son action cyber à ces groupes de « hackers patriotiques », certains semblent s'être aussi mobilisés de leur propre chef.

« Côté ukrainien » en revanche, il existe une myriade d'acteurs difficile à démêler, du fait de leur multiplicité et du caractère généralement récent de leur engagement. A des fins d'appréhension globale du paysage, on s'en tiendra ici à distinguer deux catégories principales mais pas nécessairement étanches : les groupes autonomes pro-Ukraine et/ou anti-Poutine ; les structures créées sous l'impulsion des autorités ukrainiennes et *a priori* mises au service de leurs intérêts directs. Ainsi de l'Internet Army of Ukraine, chargée de la lutte informationnelle et de la contre-propagande, et de l'IT Army, mise sur pied pour perturber le fonctionnement des systèmes d'information russes par des cyberattaques. Ces dernières consistent principalement en des dénis de service (ou DDoS, provoquant la mise hors service d'un réseau par saturation de requêtes), des défacements (modifications indésirables d'une page web), mais également des *hack & leaks* (piratages entraînant des fuites de données massives). L'IT Army se targue de rassembler 300 000 membres volontaires, un chiffre qui a été largement partagé, mais elle en compte très probablement bien moins en réalité, sans qu'il soit possible d'en déterminer le nombre exact : si l'on s'en tient à la popularité de sa chaîne Telegram, l'élan de mobilisation suscité concerne potentiellement plusieurs milliers voire dizaines de milliers de personnes.

En dehors de cette IT Army, d'autres groupes agissent de manière autonome et *a priori* sans concertation directe avec elle. Anonymous, revenu sur le devant de la scène à cette occasion, est le plus connu d'entre eux, mais des acteurs aussi divers que les Cyber-Partisans biélorusses, NB65, GhostSec, Kelvin Security, DoomSec ou AgainstTheWest sont également impliqués. Si la nature décentralisée de ces structures – et tout particulièrement de la nébuleuse Anonymous, au sein de laquelle gravitent divers groupes réunis sous sa bannière, mais avec chacun leurs modes opératoires et objectifs – rend l'attribution et l'analyse de leurs actions complexe et parfois invérifiable, il n'en demeure pas moins qu'ils semblent avoir fait preuve d'un activisme réel et intense contre les intérêts russes (entreprises, institutions et agences gouvernementales). Ces hacktivistes se lancent parfois dans des « confrontations » plus ou moins assumées avec des groupes pro-russes, à l'image de la branche italienne d'Anonymous, qui s'est déclarée « en guerre » contre Killnet.

Malgré l'ampleur des opérations, une efficacité limitée

Les opérations menées par les hacktivistes pro-ukrainiens sont donc diverses et aboutissent aussi bien à des interruptions de service, des fuites de données ciblées qu'à des publications par blocs de plusieurs téraoctets. Toute la question est de déterminer la réalité des revendications comme de l'impact produit. Si l'accumulation des attaques peut mettre sous pression les autorités russes, les contraignant notamment à reconnaître la situation délicate dans laquelle se trouvait le pays, elle les conforte aussi dans leur « syndrome de la forteresse assiégée ». Les perturbations de service, comme celle des chaînes de télévision russes ou des sites gouvernementaux, voire les interruptions, comme celle de Rutube (l'équivalent russe de Youtube), sont restées momentanées et ne semblent pas avoir dépassé le stade de la nuisance certes symbolique, mais ponctuelle. Quand certaines fuites de données ont notamment permis de lever le voile sur l'identité de soldats et d'agents des services de

sécurité russes, pouvant faciliter leur ciblage ultérieur, d'autres ont plutôt encouragé des usages « récréatifs », lorsqu'il s'agissait notamment d'harceler des agents russes dont les numéros de téléphone avaient fuité. Le tout avec une efficacité probablement limitée, mais aussi le risque de compliquer certaines enquêtes journalistiques (car les appels peuvent inciter à l'abandon ou la modification des numéros piégés), voire l'action de services de renseignement. Pour ce qui est des entreprises russes touchées, la continuité de leurs activités ne semble pas avoir été menacée jusqu'ici, en dépit des nombreuses attaques auxquelles elles font face.

Qui plus est, la publication massive de données tous azimuts, sans hiérarchisation ni filtrage, les rend de fait difficilement exploitables au regard de l'immensité de la tâche pour les enquêteurs – qu'ils soient analystes, journalistes ou simples citoyens engagés. Ce genre de manœuvre privilégiant la quantité sur la qualité révèle aussi que les hackers n'ont pas toujours été en capacité de cibler efficacement les informations de valeur au sein des réseaux qu'ils pénétraient. Les attaques menées par les hacktivistes n'ont donc – jusqu'à preuve du contraire – pas produit d'effet stratégique, ce qui ne signifie pas pour autant qu'il faille les minimiser.
Leur impact concret est peut-être à chercher ailleurs. Comme le suggère Mykhaïlo Fedorov, le vice-premier ministre ukrainien en charge de la transformation numérique, la saturation des systèmes d'information russes par les attaques pro-ukrainiennes pourrait avoir eu pour effet de fixer une partie des capacités russes, astreintes à la défense de ces réseaux plutôt qu'à la préparation d'actions cyberoffensives.

Un engagement qui laisse de nombreuses questions en suspens

Force est de reconnaître que l'hacktivisme dans le contexte actuel produit des effets indésirables. Tout d'abord, la mise à disposition – notamment sur les canaux de diffusion de l'IT Army – d'outils offensifs « clés en main » (notamment pour lancer des attaques DDoS) signifie qu'un certain nombre de néophytes peut prendre part à ces actions, mais aussi que ces outils pourront logiquement être réemployés à d'autres fins et de manière incontrôlée. Or, quand bien même leurs intentions sont louables, les hacktivistes engendrent parfois des dommages collatéraux. Ensuite, la multiplication des opérations induit une plus forte circulation d'extraits de code informatique pouvant être ultérieurement réemployés par des acteurs malveillants et *a fortiori* compliquer l'attribution de futures attaques. Le réemploi de code est parfois favorisé par certains groupes eux-mêmes, à l'image de NB65 qui s'en est pris à des actifs russes en réutilisant le code et les pratiques (hameçonnage, cryptage des données et demande de rançon) du groupe cybercriminel Conti. Enfin, les actions répétées contribuent – à tort – à nourrir les discours sur une prétendue « cyberguerre » ambiante, terme galvaudé à la pertinence en réalité limitée, mais qui concoure au renforcement des tensions.

Par ailleurs, en prenant part à ces opérations, les hacktivistes s'exposent à plusieurs risques sur le plan individuel. Tout d'abord, celui d'être victimes de manipulation : au milieu d'eux se trouvent des groupes criminels qui tentent de profiter de la situation pour revendre des jeux de données, mais aussi pour s'attaquer aux proies faciles que sont les individus peu expérimentés, mais désireux de s'impliquer. Ensuite, celui d'être victimes de représailles ciblées : si pour le moment chaque adversaire est occupé ailleurs, on ne peut écarter à terme la possibilité que la sécurité des données – voire la sécurité personnelle – de certains individus impliqués puisse être en jeu. Le risque est également d'ordre juridique, point qui soulève des interrogations aux réponses incomplètes : faut-il considérer les hacktivistes en temps de guerre comme des « cybercombattants » à part entière ? Le cas échéant, cela supposerait de les reconnaître et les accompagner comme tels, mais aussi de s'assurer qu'ils agissent dans le respect du droit international humanitaire et du droit des conflits armés (respect des principes d'humanité, discrimination et proportionnalité), lesquels imposent des critères de redevabilité et de responsabilité. L'injonction de *due diligence* pèserait dès lors sur les États, ce qui rend cette hypothèse peu probable, car trop contraignante et aventureuse. Faut-il au contraire rappeler que les actions des hacktivistes relèvent de l'illégalité et donc de la cybercriminalité ? Les individus s'exposent de fait à des sanctions pénales, non seulement de la part de Moscou, mais théoriquement aussi des Etats dont ils sont ressortissants. Doit-on considérer qu'ils relèvent d'un autre statut ou leur accorder des exemptions en raison des circonstances exceptionnelles dans lesquelles ils opèrent ? Ce serait reconnaître l'existence d'un « deux poids, deux mesures » qui nous compliquerait probablement la tâche ailleurs. Si l'option du *benign neglect* (« négligence bienveillante ») peut sembler viable jusqu'ici, rien ne dit qu'elle le demeurera indéfiniment.

La question divise les experts, et hormis la prise de position publique d'un responsable américain, les États occidentaux sont restés jusqu'ici relativement silencieux sur ces pratiques – silence qui pour Moscou vaut assentiment. Il est pourtant dans l'intérêt des États de s'en saisir davantage et de clarifier leur position, d'une part afin d'éviter de nourrir le récit russe, et d'autre part dans l'optique de ménager l'avenir, car rien ne garantit qu'ils resteront épargnés demain par ce même phénomène. Ceci suppose de sensibiliser plus directement les potentiels hacktivistes aux divers risques (juridique, économique, voire sécuritaire) auxquels ils s'exposent. Il faut également pouvoir questionner la disruption des normes ainsi engendrée, alors que les Etats

européens, dont la France au premier chef, œuvrent pour préserver la stabilité du cyberespace. L'IT Army constitue de ce point de vue un cas d'école à la fois novateur et problématique, dans la mesure où sa coordination est assurée – au moins pour partie – par un État, et où elle entretient par exemple des relations ambiguës avec un groupe cybercriminel comme IPstress (spécialisé dans les attaques DDoS). Si elle semble jusqu'ici choisir ses objectifs avec un minimum de soin et éviter de causer des dommages irréparables, elle n'en cible pas moins des infrastructures, y compris civiles. Or rien ne garantit que la structure n'échappe à l'avenir au contrôle du gouvernement ukrainien ; la question de sa pérennité ou de sa dissolution à l'issue du conflit se poserait alors avec d'autant plus d'acuité. Autant d'éléments qui devraient nous interpeler collectivement davantage.

Tout ceci soulève de fait la question de la responsabilité étatique vis-à-vis de la promotion du hacktivisme, quand bien même à des fins potentiellement « légitimes » (en l'espèce, la légitime défense). Qui plus est, la limite parfois fine entre engagement personnel et fonction professionnelle peut aussi mettre les États en difficulté, dans le cas où des agents publics mèneraient ou participeraient à des actions sur leur temps libre. La France ne doit pas s'estimer à l'abri de ce genre de débat, alors qu'un doute plane sur la nationalité de membres du groupe AgainstTheWest – lequel s'affirme proche de services de renseignement occidentaux. Les acteurs privés ne peuvent eux non plus ignorer le sujet, dans la mesure où les hacktivistes utilisent leurs infrastructures et leurs services tout en œuvrant au contournement actif des mesures de sécurité que ces mêmes entreprises mettent en place. L'enjeu est *in fine* géopolitique, car le brouillage des lignes et des responsabilités nourrit plus ou moins directement le narratif russe de « collusion » et « d'irresponsabilité » occidentale, au risque de légitimer des représailles ultérieures, y compris contre des infrastructures publiques comme privées. Tant que la maîtrise de l'escalade et la promotion des normes de comportement responsable dans le cyberespace demeurent des objectifs communément partagés, de telles opérations ajouteront à l'incertitude, et seront par conséquent susceptibles de compliquer le travail diplomatique.

Quel avenir pour l'hacktivisme en temps de conflit ?

Il est probable que, comme par le passé, l'hacktivisme s'essouffle à mesure que le conflit en Ukraine se prolonge, que la fatigue gagne l'opinion publique mondiale, que les dissensions internes aux groupes grandissent, et que le manque de résultats tangibles cesse de rendre cet engagement attractif. Pour autant, il n'est pas impossible que le phénomène ait encore de beaux jours devant lui. La « mercenarisation » du hacktivisme, d'ores et déjà amorcée en Ukraine, est ainsi un horizon possible. Revalorisé en tant que forme d'action directe, « horizontale » et visible, il pourrait être amené à jouer un rôle plus récurrent dans le cadre de futurs conflits. En un sens, c'est déjà le cas lorsque les différends demeurent sous le seuil de la conflictualité ouverte : Israël et l'Iran se livrent ainsi régulièrement à des escarmouches cyber par groupes d'hacktivistes interposés, le recours à ces derniers permettant un engagement à moindres coûts et risques pour chaque État. Enfin, la forme du hacktivisme pourrait également évoluer depuis les attaques DDoS vers davantage de rançongiciels « à caractère politique » (logiciels d'extorsion prenant en otage les données de la cible après les avoir chiffrées), ou de « proteswares » (logiciels *open source* détournés par leurs développeurs lors de mises à jour). Cette dernière tendance d'autant plus préoccupante qu'elle risque de nuire à l'ensemble de l'écosystème *open source* sur lequel reposent les fondements de notre vie numérique.

Tout comme la guerre, l'hacktivisme dans le contexte ukrainien pourrait donc durer, du moins dans les mois à venir. Seul le temps permettra de mesurer son impact, resté jusqu'ici limité dans les faits, mais porteur d'une forte charge symbolique. Si l'ampleur de la mobilisation actuelle devait « valider de fait » la légitimité comme la persistance de ce phénomène, alors l'IT Army pourrait bien incarner les prémices d'une « institutionnalisation par défaut » de l'implication de ce type d'acteurs dans de futurs conflits. Autant de raisons pour ne pas balayer d'un simple revers de main ce retour au premier plan du hacktivisme.

Les propos tenus dans cet article n'engagent ni le Centre d'analyse, de prévision et de stratégie (CAPS), ni le ministère de l'Europe et des Affaires étrangères.

Crédit : Getty Images

•— ••— — • ••— •—• •••

Benjamin Pajot

Benjamin Pajot est chargé de mission au Centre d'analyse, de prévision et de stratégie (CAPS) du ministère de l'Europe et des Affaires étrangères. Ses recherches portent sur la géopolitique du numérique et des nouvelles technologies. Il s'intéresse notamment à la rivalité technologique sino-américaine, aux enjeux de manipulations de l'information, aux communs numériques et à la dimension cyber du conflit russo-ukrainien.

Comment citer cette publication

Benjamin Pajot, « Appréhender l'hacktivisme pro-ukrainien face à l'invasion russe », *Le Rubicon*, 30 août 2022 [https://lerubicon.org/apprehender-lhacktivisme-pro-ukrainien-face-a-linvasion-russe/].