Réflexions générales sur le cybercrime et la cybersécurité, à l'aune du cas russe

Daniel VENTRE

Ingénieur de recherche, CNRS
Chercheur, CESDIP
Auteur de « Artificial Intelligence, Cybersecurity and Cyberdefense », Wiley-ISTE, Nov 2020

Quand on évoque la Russie et son lien au cyberespace, le propos est généralement peu flatteur. Le pays abriterait une cybercriminalité parmi les plus organisées, performantes et actives de la planète[1], qui parfois même bénéficierait d'un soutien actif des autorités[2], quand ces dernières ne seraient pas directement à la manœuvre. Il est également reproché à la Russie son refus d'adhérer à la Convention de Budapest et son absence de coopération en matière de lutte internationale contre le cybercrime. Mais la Russie subit elle aussi un volume important de cyberattaques qu'elle a bien du mal à prévenir ou contrer. Ses politiques de cybersécurité sont-elles capables de contenir le phénomène ?

La Russie, une cybercriminalité qui ne cesse de croître

La Russie, comme de très nombreux autres pays, fait état en 2020 d'une augmentation significative de la cybercriminalité. Cette tendance s'inscrit dans un mouvement de longue durée, amorcé dans les années 1990-2000.

La Russie enregistre officiellement plus de 510 400 cybercrimes en 2020 (soit 74% de plus qu'en 2019). La fraude à la carte bancaire a été multipliée par 6 en une année. Une très forte augmentation du nombre de cybercrimes a été observée au cours du premier semestre 2020 par rapport à la même période de 2019 : + 92%. En 2020, les délits à la carte bancaire ayant touché le pays ont augmenté de 500% par rapport à 2019. Selon une étude de Check Point, au cours du premier semestre 2020 une entreprise russe subissait en moyenne 570 attaques par semaine, soit davantage que la moyenne mondiale qui est de 474[3]. Les assauts cumulés du cybercrime auraient coûté 40 milliards d'euros à l'économie du pays en 2020.

La société russe est attaquée de deux côtés : celui de criminels dont les attaques proviennent de l'étranger, et de criminels russophones.

Les attaques de l'intérieur

Une « tendance caractéristique de la Russie est liée aux pays d'origine des attaques. Alors que dans le monde la très grande majorité des attaques proviennent d'autres pays, d'autres continents, en Russie 47% des attaques proviennent de l'intérieur du pays »[4]. Le

[1] Lucie Kadlecová, Russian-speaking Cyber Crime: Reasons behind Its Success, The European Review of Organised Crime 2(2), 2015, 104-121, https://standinggroups.ecpr.eu/sgoc/wp-content/uploads/sites/51/2020/01/kadlecova.pdf

[2] Jeffrey Carr, Inside Cyber Warfare: Mapping the Cyber Underworld, O'Reilly Media, 2009,

[3] https://www.tadviser.ru/

[4] https://www.tadviser.ru/

phénomène n'est pas nouveau. Ce marché intérieur représentait déjà en 2010-2011 environ 50% des gains de la cybercriminalité russe. Ces hackers russophones auraient dérobé en 2016 près de 30 millions d'euros à la Banque centrale russe ; cette dernière enregistrait en 2019 plus d'un demi-million d'opérations frauduleuses sur des comptes bancaires du pays, visant autant les particuliers que les entreprises.

Les attaques de l'extérieur

Selon Rostelecom[5], le SOLAR JSOC[6] (centre de surveillance et de réponse aux cyberattaques) et le SOLAR CERT (cyber-incidents) ont enregistré au cours de l'année 2020 plus de 200 attaques[7] attribuables à des hackers professionnels visant largement des pans entiers de l'économie russe. Une trentaine de ces attaques servaient probablement les intérêts d'Etats étrangers.

Des attaques contre des systèmes étatiques fragiles

La Russie est attaquée sur ses points faibles que sont les systèmes des autorités et les sous-traitants et fournisseurs : 90% des systèmes des agences gouvernementales seraient piratables sans trop d'efforts[8] ; plus de la moitié des sites institutionnels seraient en http ; et plus de 60% des organisations gouvernementales souffriraient de vulnérabilités au niveau des serveurs, des applications, systèmes d'exploitation.

… malgré une cybersécurité qui se renforce

Quand le réseau internet arrive en Russie au milieu des années 1990, le pays ne dispose pas encore, contrairement à d'autres pays occidentaux (Etats-Unis, Royaume-Uni, France...) de lois criminalisant les utilisations abusives des outils informatiques. En 1996 le Code Pénal de la Fédération de Russie comble partiellement ce vide lorsqu'il est enrichi d'un Chapitre 28 sur les crimes dans la sphère informatique, article amendé à plusieurs reprises depuis. Aujourd'hui plusieurs articles du code pénal russe (articles 138, 146, 158-160, 165, 180, 242, 272-274) permettent de sanctionner la cybercriminalité dans ses diverses manifestations (interceptions illégales, accès non autorisés, atteintes aux systèmes et aux données, vol et fraude par moyens informatiques, pédopornographie, infractions à la propriété intellectuelle, etc.) :

- Chapitre 28 du Code Pénal russe (Articles 272-274.1) (1996)[9]

- Loi pour la protection des données personnelles (2006)

- Loi Fédérale n° 187 (Juillet 2017) "sur la sécurité des infrastructures d'information critiques de la Fédération de Russie" qui définit une cyberattaque comme une menace ciblée ou un impact d'attaque logicielle ou matérielle contre un réseau de télécommunication, dans l'objectif d'altérer ou mettre un terme à son fonctionnement. L'accès non autorisé à l'information stockée protégée d'infrastructures critiques est puni de 2 à 6 ans de prison et d'une amende de 500 000 à un million de roubles (Article 274.1 du Code Pénal). Cette loi est entrée en vigueur le 1er janvier 2018.

- Loi Fédérale n° 194 (juillet 2017) : introduit la responsabilité pénale de quiconque cause dommage à l'infrastructure d'information critique (Article 274.1 du Code Pénal)

- Loi Fédérale n° 111 (avril 2018), introduit l'article 159.3 du Code Pénal (sanctions pénales pour fraude par moyens de paiement électroniques) et l'article 159.6 (fraude informatique).

---

[5] https://www.tadviser.ru/

[6] https://rt-solar.ru/products/jsoc/ https://rt-solar.ru/analytics/reports/ Ce site propose plusieurs rapports ouvrant la période 2014-2020

[7] https://rt-solar.ru/upload/iblock/c9b/Otchet-ob-atakakh-i-instrumentarii-professionalnykh-kibergruppirovok-za-2020-god.pdf

[8] https://www.tadviser.ru/

[9] https://www.wto.org/english/thewto_e/acc_e/rus_e/wtaccrus48_leg_6.pdf Traduction anglaise

A ce corpus juridique s'ajoute une organisation de la cybersécurité qui prend plusieurs formes :

- Création d'entreprises de cybersécurité (l'entreprise Group-IB créé en 2003 par Ilya Sachkov, par exemple) ;

- CERT national, d'entreprise (CERT GIB en 2011), du secteur financier (FinCERT, 2015)

- Création d'un centre national de coordination sous le contrôle du Federal Security Service (FSS), pour traiter les cyber-incidents (septembre 2018) ;

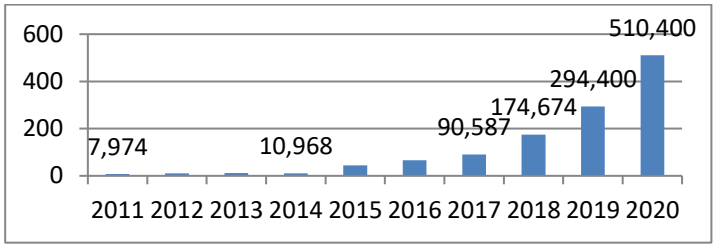
- Politiques et stratégies de cybersécurité : doctrine de sécurité de l'information[10] (2016) ; entrée en vigueur du Sovereign Internet Bill en novembre 2019 ; nouvelle doctrine de cybersécurité approuvée par le président russe Vladimir Poutine (décembre 2019) ; le Ministère de l'Intérieur russe s'est récemment doté d'une « cyber police » ; en septembre 2020 le Bureau du procureur général de la fédération de Russie a créé un groupe de travail pour la lutte contre le cybercrime, composé de représentants du Ministère des Affaires étrangères, du FSB, du Ministère de l'Intérieur et du Ministère de la Justice ;

- Initiatives internationales en matière de politiques de cybersécurité ou lutte contre le cybercrime : proposition de convention déposée par la Russie auprès de l'ONU en 2017 ; adoption par l'Assemblée générale des Nations Unies de deux résolutions proposées par la Russie (décembre 2018) ; accord « Cooperation in Combating Cybercrime » entre Etats membres de la Communauté des Etats Indépendants (CEI) (septembre 2018).

Les instruments permettant de construire la cybersécurité et lutter contre le cybercrime ne manquent donc pas vraiment à la Russie.

Quelques réflexions sur le cybercrime et la cybersécurité

Aucun indicateur ne permet toutefois d'espérer une amélioration de la situation à court ou moyen terme : l'histogramme ci-dessous illustre cette tendance croissante de la criminalité informatique en Russie.



Graphique : Nombre de crimes TIC en Russie[11]

En 2019, les cybercrimes représentaient 14,5% de l'ensemble des crimes enregistrés en Russie. Leur part n'était que de 8,8% l'année précédente[12]. D'après le Ministère de l'Intérieur russe la part des cybercrimes atteignait même 22,3% de la criminalité dans son ensemble au cours du premier semestre 2020.

La part du cybercrime ne cesse donc de gagner du terrain. En Russie, mais partout ailleurs dans le monde. Car bien sûr la situation de la Russie n'est pas isolée. Elle est au contraire assez commune : la cybercriminalité est à peu près partout en augmentation constante et ce en dépit de la somme d'efforts consentis depuis des décennies en matière de cybersécurité et lutte conte le cybercrime.

On nous rétorquera que les effets du cybercrime seraient sans doute bien plus importants en l'absence de toutes mesures pour le contenir. Mais le constat est sans appel : aucune inversion durable de l'évolution du cybercrime n'a pu être engagée et ne le sera probablement dans les années à venir.

Si l'expansion du cyberespace, l'intensification des échanges sur les réseaux, l'augmentation du nombre d'internautes mais aussi de machines connectées, sont

[10] https://www.mid.ru/en/foreign_policy/official_documents/-/asset_publisher/CptICkB6BZ29/content/id/2563163

[11] Reconstitué d'après plusieurs sources russes. https://www.ponarseurasia.org/memo/russian-itc-security-policy-and-cybercrime

[12] https://ria.ru/20200127/1563946596.html

l'un des facteurs pouvant contribuer à la prolifération du cybercrime (les opportunités criminelles sont chaque jour plus nombreuses), d'autres variables devraient pourtant participer de la réduction de l'insécurité. En effet, les « surveillants » ou « gardiens » du cyberespace sont eux aussi de plus en plus nombreux (CERTs, entreprises de cybersécurité, polices, hackers éthiques, jusqu'aux internautes mêmes contraints à la vigilance...). Quant au vivier des cybercriminels (pas tous nécessairement hackers par ailleurs), nul ne sait véritablement s'il a augmenté dans les mêmes proportions que les volumes de cybercrimes constatés. Peut-être sont-ils devenus tout simplement plus performants, sans s'être eux-mêmes multipliés.

Les instruments et méthodes utilisés ces dernières décennies, qu'ils soient juridiques, politiques, organisationnels, industriels, technologiques, se sont révélés relativement inefficaces. Faut-il par exemple voir dans l'efficacité du cybercrime les conséquences d'une militarisation accélérée du cyberespace, et qui transforme ce dernier en un lieu d'affrontements à peine masqués ?

Cet échec sécuritaire global impose quoi qu'il en soit une remise en question en profondeur.