33rd
International Workshop
on Global Security

La sécurité globale en crise:

Les fissures grandissantes dans l'ordre international fondé sur des règles, la montée de L'islam radical, la cybermenace, et l'échec de la globalisation

Sommaire et Conclusions

« Clairement, l'OTAN n'a jamais été aussi nécessaire tout en n'ayant jamais fait l'objet d'autant de menaces graves. La confiance mutuelle, qui est l'élément central de l'Alliance, doit être restaurée. Cependant, je ne suis pas convaincu que cela puissese faire. Les six prochains mois seront une période critique à la fois pour l'Alliance et aussi pour les Etats-Unis. » Général George Joulwan, USA (Ret), 11e Commandant suprême des forces alliées en Europe (SACEUR).

Conclusion 1. La sécurité globale traverse un moment de difficultés qui est en train de créer de profondes et dangereuses fissures dans l'ordre international.

Le Brexit, le triomphe inattendu de Donald Trump, la défaite du référendum Italien, et la montée de groupes politiques d'extrême droite suggèrent l'apparition de profondes fissures dans le système de sécurité international, dues en partie au rejet des effets secondaires indésirables de la globalisation (inégalités grandissantes, politiques d'austérité et flux de réfugiés) ; à la propagation du terrorisme alimenté par les groupes salafistes et wahhabites de l'islam, ainsi qu'à l'internet et autres technologies variées qui amplifient ces forces. Ces difficultés sont exploitées par la Russie, par d'autres états, par les terroristes et les groupes criminels.

Conclusion 2. Une difficulté particulièrement sérieuse tient à l'extraordinaire vulnérabilité de la plupart des organisations—sociétés multinationales, gouvernements, et organisations internationales telles que l'OTAN ou l'Union Européenne—face aux attaques cyber. Toutes ont besoin d'allouer davantage de ressources à la cyber défense et d'améliorer leur résistance cyber. Elles devront sinon en subir les conséquences.

Beaucoup de sociétés internationales, gouvernements, et organisations similaires souffrent d'un manque extrême de « cyber maturité ». En conséquence, même les plus grands géants industriels— Coca Cola, Exxon, Boeing, ou Volkswagen—et les gouvernements sont en danger.

Leurs défaillances sont telles qu'il faudrait une augmentation des ressources cyber de 100 à 150% pour recruter, former et, au final, garder les ingénieurs les plus compétents afin de corriger ces vulnérabilités dangereuses et améliorer la préparation cyber de ces organisations.

Conclusion 3. Selon des analyses effectuées par la CIA, la Russie serait intervenue dans la campagne présidentielle américaine grâce à une opération cyber massive afin d'aider son candidat préféré, Donald Trump, à gagner la présidence.

La Russie aurait monté une opération cyber très efficace visant le Comité national démocrate. L'attaque a permis d'obtenir les emails de la campagne présidentielle d'Hillary Clinton qui ont été diffusés par WikiLeaks. Etant donné que l'élection était serrée—Hillary Clinton ayant gagné le vote populaire avec une marge de près de 3 millions de votes—la Russie semble avoir influencé le résultat en faisant basculer la course électorale au profit de Donald Trump.

Il est intéressant de relever que l'élection ne semble pas avoir été décidée par le contenu des documents diffusés par les pirates informatiques Russes mais plutôt par un goutte-à-goutte incessant de fuites d'emails…aucune n'étant particulièrement compromettante…mais leur flux

constant et l'intervention du FBI que ce flux a provoqué ont donné l'impression de quelque chose de trouble et de suspect. Pire encore, de « fausses nouvelles » concernant les élections ont été amplifiées par les algorithmes de Facebook et Google et par les tweets des supporters de Trump, qui ont atteint des millions d'électeurs dans les derniers jours de la campagne.

Conclusion 4. Si l'attribution faite par la CIA est correcte, l'intervention Russe dans les élections américaines est peut-être l'une des plus graves opérations cyber jamais menées puisqu'elle a affaibli la confiance dans le système électoral. Les élections de 2017 en France et en Allemagne courent le même risque de perturbations.

L'attaque cyber russe doit être vue comme un avertissement urgent à la communauté internationale puisque la Russie est soupçonnée d'avoir aussi influencé le vote du Brexit[1] en Angleterre et les élections régionales en Allemagne. Son influence pèse également sur l'élection présidentielle en France où une banque russe finance la campagne de Marine Le Pen. Si les Etats-Unis n'ont pas réussi à stopper cette interférence, les états européens ont-ils la moindre chance d'empêcher une attaque/intervention similaire ?

Conclusion 5. Au fur et à mesure que leur califat s'affaiblit, ISIS/Daesh doit trouver d'autres moyens de monter des attaques terroristes. Par exemple, des bandes organisées de cyber criminels (cyber mercenaires) et des groupes terroristes Islamiques comme ISIS/Daesh pourraient s'associer pour monter de violentes attaques cyber.

Face à ce danger, « nous avons besoin d'une coalition de gouvernements, de citoyens, de fournisseurs de service internet, d'entreprises informatiques, et d'ONG pour lutter contre l'utilisation de la toile par les terroristes et les djihadistes. »

Il y a lieu de s'inquiéter : les mafias, liées au crime organisé et parfois même protégées par des états, ont les moyens d'exécuter des attaques extrêmement violentes ; et les groupes terroristes comme ISIS/Daesh ont de riches supporters salafistes/wahhabites qui veulent propager les attaques terroristes. Il est donc fortement probable que les cyber mercenaires et ces groupes terroristes fusionneront, si ce n'est déjà fait.

Conclusion 6. Pour faire face à ISIS/Daesh, il faut d'abord reconnaître que le djihadisme salafiste est l'ennemi qui vise la suprématie globale en remplaçant l'influence occidentale par un califat et l'usage de la violence. Pourtant, la plupart des gouvernements préfèrent actuellement accorder la priorité aux bénéfices financiers qu'ils retirent de leurs relations privilégiées avec les Etats du Golfe riches en pétrole qui continuent de financer l'islam radical.

La plupart des gouvernements et des grandes organisations internationales hésitent à attribuer les attaques terroristes toujours plus nombreuses à l'islam radical, au salafisme, ou au wahhabisme. Et ils évitent de mentionner dans les Etats du Golfe (le Koweït, le Quatar, ou l'Arabie saoudite) les sources financières de ces activités terroristes. Selon un consensus bien établi, il est préférable d'accepter la propagation du salafisme plutôt que de risquer de perdre les investissements des pays riches en pétrole ou l'accès à leurs marchés d'armement, d'aviation civile, et d'infrastructure. Un changement radical peut toutefois se produire avec l'apparition de personnalités politiques comme le candidat à la présidence en France, François Fillon, ou Donald Trump, qui proposent des mesures extrêmes pour stopper l'Islam radical dans leurs pays.

Conclusion 7. Tandis que l'opposition du public aux accords commerciaux (TTIP, ACS/TISA, ALENA/NAFTA) semble avoir été une motivation essentielle derrière le Brexit et d'autres bouleversements politiques, certaines provisions de ces traités peuvent aussi avoir des conséquences sur la cyber sécurité : elles peuvent limiter ou même bloquer la capacité des

[1] Newsweek. Opinion. « Is the Brexit Vote Legitimate If Russia Influenced the Outcome? » Baylon, Caroline. 12/2/16 at 4:32 AM

pays à imposer des standards de cyber sécurité qui sont essentiels pour protéger leurs citoyens.

Les retombées cyber sécuritaires d'accords commerciaux comme TTIP, TISA, ou NAFTA sont mal connues. Les dispositions sur la protection des investisseurs de ces accords vont-elles limiter ou bloquer la capacité des pays à imposer des standards de cyber sécurité comme ceux que ANSSI considère essentiels en France ? Vont-elles empêcher les pays d'imposer des critères de localisation afin de pouvoir conserver certaines données critiques à l'intérieur des frontières nationales ?

Conclusion 8. Le développement exponentiel de l'Internet des objets (IoT/IdO)—avec bientôt 50 milliards d'objets connectés—introduit de vastes failles de sécurité qui vont de la cybercriminalité jusqu'aux attaques cyber sur l'infrastructure critique. (Une attaque malveillante Mirai a récemment exploité le manque de protection de 100.000 objets, comme par exemple des caméras de surveillance, pour fermer une partie de l'internet.

Etant donné que Mirai a pu provoquer une attaque massive par déni de service (DDoS) de 1 téraoctet par seconde en utilisant 100.000 caméras de sécurité connectées à l'internet, une attaque de 10 teraoctet par seconde ne peut pas être bien loin derrière. Des attaques encore plus grandes ayant le potentiel de fermer une grande partie du réseau internet pourraient suivre. Un botnet Mirai peut actuellement se louer pour 7.500 euros par semaine, et le dark web vante déjà la possibilité d'acheter un botnet de 400.000 objets connectés.

Conclusion 9. Les gouvernements ne peuvent plus compter sur les forces du marché pour protéger leurs sociétés. Cette approche a échoué. Ils doivent plutôt travailler avec l'industrie pour développer des normes capables de protéger l'internet et leurs citoyens d'attaques encore plus importantes. Quant à la menace terroriste, elle demandera probablement une action coordonnée OTAN, UE et ONU.

Chaque pays devra mobiliser ses citoyens en matière de sécurité cyber en organisant une grande campagne cyber dans les écoles et auprès du public et en nommant un ministre responsable pour la cybersécurité. Il faudra également des cours cyber pour former des dizaines de milliers de cyber professionnels. Etant donné la gravité des dangers, faudra-t-il passer un test semblable à un permis de conduire pour avoir le droit d'utiliser l'internet ?

Conclusion 10. L'impact social, économique, et politique sur nos sociétés est ce qui compte le plus—un patient dans un hôpital dont l'opération est bloquée, une société de télécommunications qui perd plus de 100.000 clients à la suite d'une attaque cyber, un pays comme l'Ukraine dont le réseau électrique est coupé, ou un pays comme l'Allemagne qui signale la perte de plus de 1% de son PIB. Et pour la première fois maintenant, les citoyens américains sont en train de perdre confiance dans leur gouvernement puisqu'un autre pays se serait immiscé dans leurs élections.

Note : Les conclusions ci-dessus ne tiennent pas compte de certaines influences qui n'étaient pas bien comprises au moment du workshop—comme le rôle des « fausses nouvelles » dans les élections et référendums, ou les effets nuisibles des médias sociaux qui accélèrent leur diffusion. Il faudra mettre en place des stratégies pour limiter ces effets avant que d'autres pays ne soient atteints.

Préparé par:
Roger Weissinger-Baylon, Ph.D. et Anne D. Baylon, LLB, MA
Center for Strategic Decision Research
Courriel: roger@csdr.org anne@csdr.org
Site web: https://www.csdr.org

The *33rd International Workshop on Global Security* is presented by Center for Strategic Decision Research (CSDR) and Institut des hautes études de défense nationale (IHEDN), with the sponsorship of the following governments and organizations:

MAJOR SPONSORS

ASSOCIATE SPONSORS

ACKNOWLEDGEMENTS TO PAST HOST AND SPONSOR GOVERNMENTS

Czech Republic
Kingdom of Denmark
Federal Republic of Germany
Republic of Hungary
Kingdom of the Netherlands
Kingdom of Norway
Republic of Greece
Republic of Poland
Republic of Portugal
Ministry of Defense of Austria
Ministry of Defense of France
Ministry of Defense of Italy
Ministry of Defense of Turkey
Canadian Armed Forces
Russian Federation's Ministry of Industry, Science & Technology