Projet de recherche n°8: Cyber-terrorisme: quels risques, quels scénarios?

Contexte

Les**risques systémiques du cyberespace** sont particulièrement préoccupants. Les **cyberoffensives**ont actuellement un avantage considérable sur les systèmes de cyberdéfense en termes d'**énergie** et de **coûts de développement**, les forces militaires classiques sont désavantagées en matière de cyber-résilience et les infrastructures critiques, notamment énergétiques et financières, sont **extrêmement vulnérables aux cyber-attaques**[1]. L'**inter-connectivité** des réseaux numériques augmente également particulièrement le risque de **diffusion** et de **contamination globale**. Les dommages causés par la dernière génération de virus **Spectrum** illustrent ce danger imminent. Les groupes armés terroristes ont perçu ces opportunités: leur **fragmentation géographique** et la **résurgence de certaines branches d'Al-Qaïda** (AQPA), historiquement innovantes, ou l'amélioration de la sécurité de lieux sensibles tels que les aéroports, pourraient constituer des **incitations contextuelles** à l'investissement dans le cyberdjihad.

Les véritables progrès scientifiques dans le domaine du cyberespace échappent au contrôle d'organisations telles qu'Al-Qaïda ou de l'Etat Islamique. Les révélations de Snowden ont montré que la NSA disposait de **capacités techniques extrêmement avancées en matière de déchiffrement de systèmes cryptographiques**[2]. Ainsi, si un scénario de s**uprématie d'organisations terroristes** dans le cyberespace est peu probable, il est tout à fait possible d'acquérir une **capacité importante de nuire et de répandre la terreur**, à la fois par l'acquisition de **nouvelles ressources financières et opérationnelles** et grâce à ces avancées technologiques. Les différentes composantes du scénario de développement du cyberdjihad[3] nécessitent une **surveillance approfondie**, et nécessairement **interfonctionnelle**,**du capital humain, des capacités techniques, des stratégies spécifiques ou des opportunités** identifiées par les groupes terroristes armés[4]. Chacune de ces composantes est en soi une question de recherche associée à cet enjeu crucial pour les États.

Le cyberespace, instrument du djihad

Il est à noter qu'«Al-Qaïda dans la péninsule arabique», un groupe pionnier dans l'utilisation de l'Internet, avait **une stratégie presque opposée** (à l'appel de combattants du djihad à venir en Syrie, NDLR): ils ont exhorté leurs partisans à **rester chez eux**. De même, Al-Qaïda et l'État Islamique pourraient encourager leurs partisans à lancer des cyberattaques depuis leur salon contre des **cibles spécifiques**(petites administrations, hôpitaux, sociétés privées).

Comment?

> En utilisant les moyens disponibles sur Internet: des **«cyber-kits»** standard du type de **logiciels malveillants «clé en main»**(comme c'est déjà le cas avec les ransomwares) à usage terroriste.
> En construisant / développant des **cellules de cyber-djihad** à partir d'ingénieurs déjà présents dans leurs rangs et recrutés exprès, au moyen de**techniques de propagande ciblées**.
> En acquérant des «**super-machines»**offrant aux GAT la possibilité de casser des systèmes par force brute, en particulier le **cryptage d'état ou ISS**, puis d'utiliser les données et connaissances ainsi obtenues pour de multiples utilisations.[5]

En obtenant de **nouvelles sources de financement**et de **nouveaux vecteurs pour transférer des fond**s à travers le monde, entre katibas, supporters, cellules de recrutement et opérationnelles.
Par le partage de **ressources informatiques** et le **soutien d'individus ou d'institutions** au djihad en rendant leur puissance de calcul disponible sur un modèle de type**BOINC**[6]: là encore, le **sentiment d'impunité** et de **gravité mineure** de chaque action isolée peut convaincre, même les personnes endoctrinées faible ou fragile puisqu'il s'agirait d'un support passif et non d'une attaque active. Les deux moyens mentionnés ci-dessus peuvent être combinés.

Pourquoi?

Ces moyens sont faciles d'accès, peu coûteux, ne nécessitent pas de connaissances spécifiques et présentent un **potentiel élevé de nuisance**s'ils sont utilisés spécifiquement contre des **cibles stratégiques** ou **en masse**sur des **cibles de moindre importance**: cela peut entraîner une **perturbation massive** des petites installations, des services publics ou privés, mais dont l'accumulation générerait de **multiples perturbations** ... L'**effet de terreur** généré est donc très important.

Intérêts en relation avec les attaques "classiques":

Les cyber-attaques ne nécessitent **aucun équipement "sensible"**(illégal ou dangereux): une simple connexion Internet suffit, ainsi que des connaissances de base (par exemple, où trouver ces cyber-kits) – connaissances qui peuvent potentiellement être mises à disposition par le groupe pour faciliter l'accès à ce genre d'attaques: **«Vademecum de la cyber-attaque à l'usage du djihadiste débutant»**.
Les cyberattaques présentent un **risque très faible**. Un sentiment d'impunité existe parce que l'arsenal juridique n'est pas bien adapté à la répression de ce type d'action (**les peines encourues sont négligeables ou inconnues** par rapport aux agressions physiques). Il existe ensuite une **facilité narrative** inhérente à ces attaques qui en encourage l'exécution, c'est-à-dire qu'en cas d'arrestation, il est facile de **plaider la naïveté** ou l' **ignorance de la portée de l'acte.**
Les cyberattaques présentent de nombreux avantages pour les **GAT**, car les données obtenues peuvent, par exemple, leur permettre : a) de perturber le fonctionnement des institutions publiques; b) de rançonner des organisations publiques ou privées; c) d'obtenir des crypto-monnaies pour**financer le djihad «sur le terrain»**; d) de rendre publiques des informations confidentielles / secrètes de la défense; (e) ou encore d'**alimenter la propagande djihadiste** en exposant des**stratégies de collusion** publiques ou non publiques, en nourrissant les **théories du complot** utilisées dans le recrutement de nouvelles recrues, en révélant des stratégies considérées comme **«impures»** ou comme faisant partie d'une **«dégénérescence» de sociétés non islamiques**...

---

[1] Baumard, Ph. , « Deterrence and escalation in an Artificial Intelligence Dominant Paradigm : Determinants and Outputs », MIT International Conference on Military Cyber Stability, MIT CSAIL Computer Science and Artificial Intelligence Laboratory. 13/12/2016

[2] Jeff Larson, "Revealed: The NSA's Secret Campaign to Crack, Undermine Internet Security", Propublica, 5 septembre 2013.

[3] Cockayne, James and Roth, Amanda (2017) "Crooked States: How organized crime and corruption will impact governance in 2050 and what states can – and should – do about it now", United Nations University.

[4] J.M. Berger, "The Evolution of Terrorist Propaganda: The Paris Attack and Social Media," Testimony to the House Committee on Foreign Affairs, pages 42-45, 27 janvier 2015.

[5] Schori Liang Christina. "Cyber Jihad : Understanding and Countering Islamic State Propaganda". February 2015, GCSP Policy Paper 2015/2

[6]Outil de calcul BOINC.

https://esd.cnam.fr/projets-de-recherche-cooperation-scientifique/projets-de-recherche/projet-de-recherche-n-8-cyber-t