Décembre 2011

Fiche de l'Irsem n°11

Cyberterrorisme : quel périmètre ?

Alix DESFORGES

Pour citer ce document :

Alix DESFORGES, " *Cyberterrorisme : quel périmètre ?"*

Fiche de l'Irsem n° 11,
décembre 2011, 7 pages

http://www.irsem.defense.gouv.fr

Décembre 2011

La notion de cyberterrorisme est apparue sous la plume de Barry Collin en 1996 qui le définit comme « *la convergence du monde physique et du monde virtuel* ». Cependant, comme pour le terrorisme, aucun consensus n'a émergé autour de la définition de son dérivé. Il existe un flou académique autour de la notion de cyberterrorisme observable dans de nombreux ouvrages et articles. Deux tendances se dégagent :

1) ceux qui considèrent que le cyberterrorisme doit regrouper l'ensemble des pratiques en ligne des groupes terroristes et

2) ceux qui estiment que le terme doit être restreint à un type d'attaques précis, celles qui utilisent le réseau Internet comme arme et/ou cible.

- B. Collin, « The Future of CyberTerrorism : Where the Pysical and Virtual Worlds Converge », *11th Annual International Symposium on Criminal Justice Issues*, 1996.

I- De l'usage d'Internet chez les groupes terroristes

a. Un quasi-consensus sur les usages

Des nombreuses études dressent la liste des « usages » d'Internet par les groupes terroristes. Les travaux de Steve Furnell et Matthew Warren, Maura Conway ou encore Gabriel Wiemann convergent à de nombreux points. Ils estiment que l'essentiel de ces usages ne sont pas spécifiques aux pratiques des groupes terroristes mais sont également partagé par des groupes politiques comme la communication (interne et externe), le recrutement, le financement, l'organisation etc. Si les termes utilisés par chacun divergent, ils désignent en fait la même pratique. Par exemple, le terme *data mining* utilisé par Gabriel Weimann recouvre les mêmes éléments que le terme *information gathering* mentionné par Timothy Thomas. Ce dernier a créé une nouvelle notion pour désigner l'ensemble des pratiques en ligne des groupes terroristes : le *cyberplanning* qu'il définit comme « *la coordination numérique d'un plan intégré* ».

Décembre 2011

- M. Conway, "Cyberterrorism: Academic Perspectives." *3rd European Conference on Information Warfare and Security*, 2004, p. 41-50.
- M. Conway, « Terrorist "use" of the Internet and Fighting Back », *Information and Security, An International Journal*, vol. 19, 2006, p. 9-30.
- G. Destouche, *Menace sur Internet: des groupes subversifs et terroristes sur le net*, Paris, Edition Michalon, 1999.
- S. Furnell et M. Warren, « Computer Hacking and Cyber terrorism : the Real Threats in the New Millenium », *Computers and Security*, vol. 18, n°1, 1999, p. 30-32
- D. Gray et A. Head, « The Importance of the Internet to the Post Modern Terrorist and its Role as a Form of Safe Heaven », *European Journal of Scientific Research*, vol.23, n°3, 2009, p. 396-404.
- S. Lawson, « The Cyber-Intifada: Activism, Hactivism, and Cyber-Terrorism in the Context of the "New Terrorism". », Séminaire *Information Warfare and Security*, Georgetown University, Automne 2001.
- T. Thomas, « Al Qaeda and the Internet: the Danger of "Cyberplanning" », *Parameters*, printemps 2003, p.112-123.
- G. Wiemann, *www.terror.net – How Modern Terrorism Uses the Internet*, Washington DC, US Institute of Peace, 2004.
- G. Wiemann, *Terror on the Internet: The New Arena, The New Challenge*, Washongton DC, 2006

b. Un désaccord quant au périmètre de définition

Certains auteurs souhaitent que le terme cyberterrorisme regroupe l'ensemble des activités terroristes sur Internet. Evan Kohlman justifie cet emploi du terme cyberterrorisme en arguant qu'il n'y a aucune distinction entre terroristes numériques et terroristes dans le monde réel. Le Conseil de l'Europe mentionne le cyberterrorisme comme étant « l'usage d'Internet pour des objectifs terroristes ». James Lewis donne un autre périmètre au cyberterrorisme qu'il définit comme « *l'utilisation des outils du réseau informatique pour renverser une infrastructure critique pour un Etat ou contraindre ou intimider un gouvernement ou la population civile* ». Dans cette définition floue, il concentre ainsi les deux courants de l'utilisation du terme cyberterrorisme. S'il évoque clairement l'emploi du réseau comme une arme ; il mentionne également toute utilisation « *des outils du réseau informatique* » pour « *contraindre ou intimider un gouvernement ou une population civile* ». Il faut cependant noter que l'emploi du terme cyberterrorisme pour désigner l'ensemble des pratiques en ligne des groupes terroristes est prôné par peu d'auteurs et ne constitue pas le principal point de désaccord au sein de la communauté des chercheurs.

- E. Kohlmann, « The real Online Terrorist Threat », *Foreign Affairs*, octobre-novembre 2006.
- Conseil de l'Europe, *Cyberterrorism: The Use of the Internet for Terrorist Purposes*, Conseil de l'Europe, 2007.

c. Un vocabulaire spécifique pour les réseaux terroristes djihadistes

Pour marquer la différence d'utilisation du terme cyberterrorisme évoqué précédemment, certains auteurs préfèrent créer et utiliser de nouveaux termes plus spécifiques pour l'étude des réseaux terroristes djihadistes, mettant volontairement de côté l'emploi de cyberterrorisme. Les termes e-djihad ou cyber-djihad sont largement répandus pour désigner les pratiques en ligne d'Al-Qaïda et de ses réseaux. La création de ces termes est justifiée par l'utilisation centrale d'Internet dans ces réseaux, ce qui n'est pas forcement le cas au sein d'autres groupes terroristes. De fait, les réseaux terroristes djihadistes font ainsi l'objet de la majorité des études portant sur l'utilisation d'Internet par les groupes terroristes.

- G. Bunt, *Islam in the Digital Age: E-Jhad, Online Fatwa sans Cyber Islamic Environnements*, London, Pluto Press, 2003.
- B. Davis, « Ending the Cyber Jihadi Combating Terrorist Exploitation of the Internet with the Rule of Law and Improved Tools for Cyber-governance », *Commlaw Conspectus*, vol. 15, 2006, p. 119-186.
- J.P. Filiu, « Les dynamiques du « cyberjihad » », *Questions Internationales*, n°47, janvier-février 2011, p. 55-59
- H. Rogan, « Abu Reuteur and the E-jihad – Virutal Battle Fronts from Iraq to the Horn of Africa », *Journal of International Affairs*, été/automne 2007, p. 89-96

Parmi les usages d'Internet par les groupes terroristes listés par les chercheurs, on retrouve chez la majorité la question de l'utilisation d'Internet comme arme et/ou cible. C'est cet usage précis que certains auteurs qualifient de cyberterrorisme.

II- Des attaques informatiques comme cyberterrorisme

a. Quel type d'attaque informatique ?

Si la majorité des auteurs se situent dans cette position de considérer le cyberterrorisme comme relevant uniquement du champ des attaques informatiques, tous ne considèrent pas le même niveau ou le même type d'attaque comme relevant du cyberterrorisme. Les difficultés de définition du périmètre du cyberterrorisme se concentrent sur cette problématique. L'impact d'une attaque et sa motivation font partie des critères discriminants pour la qualification d'une attaque informatique comme un acte de

Décembre 2011

cyberterrorisme chez certains auteurs. Dorothy Denning considère que le cyberterrorisme est « *une attaque informatique ou menace d'attaque informatique entrainant d'importants dégâts conduite par des acteurs non étatiques contre des systèmes d'information pour intimider ou contraindre des gouvernements ou sociétés dans le cadre d'objectifs d'ordre politique ou sociaux* ». De son côté Mark Pollitt le définit comme « *une attaque préméditée et politique motivée contre les systèmes d'information, programmes informatiques et données par des sous groupes nationaux ou agent clandestin de laquelle résulte des actes de violence contre des cibles non combattantes* ».

Ces deux exemples témoignent de la diversité des définitions existantes pour le cyberterrorisme. La prise en compte de certains paramètres tel que le niveau de technicité de l'attaque est importante car elle peut conduire pour certains auteurs à réévaluer le périmètre des acteurs concernés par le cyberterrorisme. Certains auteurs vont en effet juger que des attaques de « faible intensité » peuvent être considérer comme du cyberterrorisme. On voit par exemple dans les exemples de définition donnés ci-dessus que les actions du groupe Anonymous relève bel et bien du cyberterrorisme selon Mark Pollitt alors que la définition de Dorothy Denning considérera que leurs actions n'impliquant pas « d'importants dégâts », elles ne peuvent être considérées comme cyberterroristes. Dorothy Denning fait d'ailleurs clairement la distinction entre le hacktivisme et le cyberterrorisme. Elle qualifie le hacktivisme comme couvrant « *des opérations utilisant les techniques de hacking à l'encontre de sites internet dans l'intention de perturber le fonctionnement normal mais sans causer de dégâts sérieux* ».

- J. Arquila, D. Ronfelt et M. Zanini, « Networks, Netwar and Information-Age Terrorism », *Countering the New Terrorism*, Santa Monica, RAND Corporation, p. 39-84.
- R. Choi et al., *Cyberterror – Prospects and Implications*, Monterey, Center for the Study of Terrorism and Irregular Warfare, Naval Postgraduated School, 1999.
- M. Conway, « Hackers as Terrorists? Why it Doesn't Compute », *Computer Fraud and Security* 203, n°12, Décembre 2003, p. 10-13.
- M. Conway, « Privacy and Securty Against Cyberterrorism », *Communications of the ACM*, vol.54, n°2, février 2011, p. 26-28
- D. Denning, « Terro's Web : How the Internet is Transforming Terrorism », *Handbook on Internet Crime*, Edition Willan, 2009.
- D. Denning, « A view of Cyberterrorism Five Year Later », *Internet Security: Hacking, Counterhacking, and Society*, Boston, Edition Jones and Bartlett, 2006.
- D. Denning, « Activisme, Hacktivism, and Cyberterrorism: The Internet as a Tool for Influencing Foreign Policy », *The Computer Security Journal*, vol. 16, n°3, été 2000, p. 15-35.
- J. Lewis, *Assessing the Risks of Cyber Terrorism, Cyber War and Other Cyber Threats.*, Washington, DC, Center for Strategic and International Studies, 2002.
- M. Pollitt, « Cyberterrorism: Fact or Fancy? », *Computer Fraud and Security*, no. 2, 1998, p. 8-10.

b. Intérêts et capacités des groupes terroristes à mener des attaques informatiques

La question des intérêts et des capacités de groupes terroristes à mener ce type d'attaque fait également débat au sein de la communauté des chercheurs. Pour certains, l'intérêt des attaques informatiques par les réseaux terroristes réside dans le ratio coût/bénéfice pour l'organisation terroriste. Pour un coût d'attaque extrêmement bas, le groupe terroriste peut obtenir un bénéfice potentiellement élevé. Pour Sam Berner et Maura Conway néanmoins, les terroristes ne possèdent pas les compétences requises pour mener des attaques informatiques qui serviraient leur agenda politique. En effet, pour garantir un certain impact, l'attaque informatique doit être de grande ampleur et donc plus difficile à mener.

Certains auteurs dont Steven Bucci évoquent l'association des sphères terroriste et cybercriminelle pour mener des attaques informatiques d'envergure fournissant ainsi les compétences nécessaires aux groupes terroristes. Barbara Mantel et James Lewis s'inquiètent de voir des attaques informatiques réalisées en coordination d'attaques physiques. Sans avoir besoin d'une grande sophistication, elles peuvent constituer un élément d'une attaque terroriste et permettre par exemple la désorganisation des secours. Pour Dorothy Denning, de tels scénarios sont inenvisageables car elle estime que « *les terroristes n'intègrent pas des modes d'attaques multiples* ». Pour elle, dans un futur proche « *les bombes restent une menace plus importante que les bytes* ».

- S. Berner, « Cyber-Terrorism : Reality or Paranoia ? », *South African Journal of Information Management*, Mars 2003.
- B. Mantel, « Terrorism and the Internet, Should Web Sites that Promote Terrorism be Shut down ? », *CQ Researcher*, Novembre 2009, p. 129-153.

c. Cyberterrorisme : mythe ou réalité ?

Selon les considérations des auteurs, on note que le niveau de la menace estimée varie. Dorothy Denning estime, comme Maura Conway, que le cyberterrorisme ne constitue qu'une faible menace et demeure aujourd'hui encore une hypothèse. Ces auteurs dont fait également partie Brian Jenkins, préfèrent rappeler que le principal danger de l'utilisation d'Internet par des groupes terroristes se situe davantage dans la propagande, qui permet une radicalisation autonome voire l'émergence d'individus organisant seul des attentats terroristes résumé dans le concept de « *lone wolf* ». Pour eux, le succès dans les médias du terme cyberterrorisme a masqué la réalité des pratiques. Maura Conway explique ce succès médiatique par la formation même du terme cyberterrorisme qui est « *l'alliance des deux plus grandes peurs : la peur de la technologie et la peur du terrorisme* ».

Décembre 2011

- B. Jenkins, *Would Be Warriors – Incidents of Jihadist Terrorist Radicalization in the United States since septembre 11, 2001*, Occasional Paper, Santa Monica, RAND Corporation, 2010.
- B. Jenkins, *Stray Dogs and Virtual Armies – Radicalization on recruitment to Jihadist Terrorism in the United States since 9/11*, Occasional Paper, Santa Monica, RAND Corporation, 2011.
- R. Pantucci, *A Typology of Lone Wolves: Preliminary Analysis of Home Islamist Terrorists*, London, The International Center for the study of radicalization and political violence, 2011.

CONCLUSION

La palette de définitions du cyberterrorisme disponible à ce jour est le reflet de la situation complexe de l'utilisation des réseaux informatiques par des groupes terroristes. Les rivalités quant à la définition du périmètre du cyberterrorisme témoignent cependant de l'angoisse réelle des Etats de voir leur bon fonctionnement altéré par des attaques informatiques et au delà de la prise de conscience des potentielles faiblesses que constituent la dépendance aux systèmes informatiques.