L'INTERGOUVERNEMENTALITÉ DANS LE CYBERESPACE : ÉTUDE COMPARÉE DES INITIATIVES DE L'OTAN ET DE L'UE

Vincent Joubert et Jean-Loup Samaan

La Découverte | *Hérodote*

2014/1 - n° 152-153
pages 261 à 275

ISSN 0338-487X

L'intergouvernementalité dans le cyberespace : étude comparée des initiatives de l'Otan et de l'UE

Vincent Joubert[1] *et Jean-Loup Samaan*[2]

Le cyberespace est aujourd'hui devenu un dossier incontournable des grandes rencontres internationales. Autrefois réservé à un public de techniciens, le sujet fait à présent partie intégrante de l'agenda diplomatique. Or, si de nombreux travaux ont ces dernières années étudié et analysé l'adaptation des États à ce nouveau phénomène, peu d'articles ont été consacrés à ce jour au rôle des organisations internationales. Dans cette perspective, il est particulièrement intéressant de se pencher sur le « traitement » de la question cyberdéfense par des acteurs tels que l'Otan et l'Union européenne.

Une étude comparée de cette mise à l'agenda du cyberespace au sein de deux organisations intergouvernementales dévoile les logiques de bureaucratisation mais aussi les limites de l'approche multilatérale. En se fondant sur un travail d'archives et une série d'entretiens conduits avec des responsables de l'Otan et de l'UE, cet article se propose d'explorer cet effort de mise en œuvre de politiques intergouvernementales dans le domaine de la cyberdéfense. Pour ce faire, nous présentons tout d'abord les efforts conduits au sein de l'Otan puis de l'UE. Puis, dans une dernière section, nous soulignons quelques-uns des écueils communs aux deux organisations dans cette entreprise d'institutionnalisation du cyberespace à l'échelle intergouvernementale.

Hérodote, n° 152-153, La Découverte, 2e trimestre 2014.

1. Doctorant à l'Institut français de géopolitique (Paris-VIII) et chargé d'études à la Fondation pour la recherche stratégique.

2. Maître de conférences au Collège de défense de l'Otan (Rome, Italie).

La cyberdéfense dans l'Otan : institutionnaliser pour exister ?

La littérature consacrée à la cyberdéfense dans l'Otan fait généralement remonter la prise de conscience de l'Alliance atlantique quant au sujet à la guerre du Kosovo en 1999 [Healey et Van Bochoven, 2012 ; Joubert, 2012 ; Hegenbart, 2013]. Au cours de la campagne aérienne conduite par les Alliés, des hackers se revendiquant de la cause serbe piratent les messageries et le site Internet du quartier général de l'organisation. Tout au plus, les pirates informatiques réussissent à réaliser un défacement de la page Web du SHAPE (Supreme Headquarters Allied Powers Europe) et des attaques de déni d'accès sur le site général de l'Otan. Les responsables de la communication de l'Alliance ont encore en souvenir l'impossibilité d'utiliser le site Internet durant plusieurs jours[3].

Ce premier cas d'attaques est relativement modeste et n'affecte pas directement la conduite des opérations militaires. Pour autant, il conduit à une autre prise de conscience, peut-être plus importante, au sein de l'Otan : l'absence d'organisation centralisatrice pour l'ensemble des réseaux opérés par l'organisation. Suite aux cyberattaques de 1999, le commandant suprême des forces alliées en Europe, le SACEUR (Supreme Allied Commander Europe), procède à un audit qui conclut que l'Alliance travaille avec pas moins d'une soixantaine de réseaux sans système de coordination ni encore moins de procédures de sécurité standardisées. « Tout était fait sur une base *ad hoc* ! » témoigne un des responsables interrogés[4].

Le diagnostic du SACEUR alarme les représentants nationaux de l'organisation qui décident pour la première fois, lors du sommet des chefs d'État à Prague en novembre 2002, d'évoquer le sujet et de le mentionner dans la déclaration finale. Les chefs d'État réunis pour le Conseil de l'Atlantique nord s'engagent à « renforcer [leurs] capacités de défense contre les cyberattaques[5] ». La formule est pour le moins succincte et le dossier apparaît bien dans l'ombre d'autres problématiques énoncées dans le document telles que la lutte contre le terrorisme ou contre la prolifération balistique et nucléaire. La cyberdéfense est aussi au programme de l'« Engagement capacitaire de Prague », un document par lequel les pays membres s'engagent à améliorer leurs ressources militaires dans des domaines circonscrits : « défense contre les armes chimiques, biologiques, radiologiques, nucléaires, renseignement, surveillance et acquisition d'objectifs[6] ».

3. Entretien téléphonique des auteurs avec un haut fonctionnaire de l'Otan, octobre 2013.

4. Entretien téléphonique des auteurs avec un haut fonctionnaire de l'Otan, octobre 2013.

5. Déclaration du sommet de Prague diffusée par les chefs d'État et de gouvernement participant à la réunion du Conseil de l'Atlantique nord tenue à Prague, 21 novembre 2002. Disponible à : <www.nato.int>.

6. Engagement capacitaire de Prague (PCC). Disponible à : <www.nato.int>.

Hérodote, n° 152-153, La Découverte, 2e trimestre 2014.

En réalité, à ce stade, le sujet est encore traité sous un angle technique. Autrement dit, il génère un consensus manifeste mais ne suscite pas pour autant un sentiment d'urgence au niveau politique. L'année suivante, en 2003, l'Otan passe un contrat avec Finmeccanica et d'autres sous-contractants pour mettre en place la *NATO Computer Incident Response Capability* (ou, en français, « Capacité Otan de réaction aux incidents informatiques » (CIRT) qui se focalise sur la détection et la réponse à des incidents informatiques. Installée à Mons, la CIRT passe en phase « opérationnelle initiale » en 2006. Elle est déclarée entièrement opérationnelle en 2013. La CIRT dispose d'un mandat purement défensif et ne peut donc s'apparenter à ce que d'aucuns appelleraient un Cyber Commandement.

Cependant les années suivantes voient le sujet clairement évoluer et passer du traitement technique à la mise sur l'agenda politique de l'Otan. Ce sont les cyberattaques de 2007 contre l'Estonie qui accélèrent les choses. Le 27 avril 2007, un flux hors du commun de messages électroniques est envoyé aux sites gouvernementaux de l'État estonien. Les attaques mènent à une congestion électronique telle qu'une *Computer Emergency Response Team* (en français CERT, voir lexique en début de volume). En vain : les sites Internet sont progressivement fermés, certains pour quelques heures, d'autres pour plusieurs jours, conduisant à une paralysie des services publics estoniens pendant trois semaines.

L'enquête qui suit est décevante et il s'avère impossible de déterminer une entité clairement responsable. En effet, les attaques proviendraient de plus de cinquante pays. Cependant, les soupçons se tournent rapidement vers la Russie : quelques semaines avant les attaques, le Parti de la réforme, vainqueur des dernières élections en Estonie, avait promis de déplacer la statue du soldat de bronze soviétique, héros de la Seconde Guerre mondiale, mais assimilé majoritairement par la population à l'occupation russe. Or, la présence d'une importante minorité russophone (près de 25 % de l'Estonie) accroît les tensions autour de cette volonté du gouvernement de Tallinn de tirer un trait sur un pan de son histoire contemporaine.

La veille des cyberattaques, une émeute démarre entre nationalistes estoniens et factions prorusses. Souhaitant préserver la paix sociale, le gouvernement déplace le soir même la statue vers un endroit plus discret, dans le cimetière militaire de Tallinn. À partir de cet instant, le conflit se propage dans le cyberespace. Rapidement après les faits, l'Estonie affirme que les codes informatiques à l'origine des attaques auraient été écrits sur des claviers en alphabet cyrillique [Clarke et Knake, p. 15]. Quelques semaines après, le secrétaire de l'US Air Force, Michael Wynne, affirme que « la Russie semble être la première à s'être engagée dans la cyberguerre » [Grant, 2007]. Jaak Aaviksoo, ministre estonien de la Défense, va plus loin en évoquant « la véritable troisième guerre mondiale[7] ».

7. Communiqué du ministère de la Défense estonien, « Internet : XXI century battlefield », 16 juin 2007.

En Europe et Amérique du Nord, se pose la question de la réponse à apporter à de telles cyberattaques dans le futur. En tant que membre de l'Otan, l'Estonie pouvait-elle invoquer l'article 5 du traité de l'Atlantique nord, appelant l'ensemble des membres de l'Alliance à répondre, si besoin militairement, à une menace touchant un allié[8] ? Et si oui, quelles auraient été les modalités de cette réponse ? Une contre-attaque informatique ou une riposte conventionnelle (*via* des moyens aériens, terrestres ou navals) ? Les mois qui suivent voient donc l'Otan s'activer sur le dossier.

En janvier 2008, la première politique de cyberdéfense (*Cyber Defense Policy*) est adoptée par le Conseil de l'Atlantique nord, signe que le sujet est désormais traité au plus haut niveau. Au sommet de Bucarest en avril de la même année, deux nouveaux organismes sont créés. L'Autorité de coordination de la cyberdéfense (*Cyber Defense Management Authority*) a désormais un bureau à Bruxelles chargé de coordonner les réponses des Alliés à de potentielles cyberattaques. Par ailleurs, le Centre d'excellence de cyberdéfense de l'Otan est constitué en Estonie le 16 mai 2008 afin de conduire des recherches et organiser des conférences pour explorer les dimensions stratégiques et légales de la question.

Puis advient la guerre russo-géorgienne. Suite à des accrochages en juillet 2008 entre des rebelles d'Ossétie du Sud et l'armée géorgienne, celle-ci envahit la région autonome le 7 août. Ce mouvement est immédiatement suivi d'une intervention russe pour contrer l'avancée géorgienne. Alors que l'armée russe avance en Ossétie du Sud, des cyberattaques ciblent les sites des médias géorgiens et les serveurs gouvernementaux. La page Web du président géorgien, Mikhaïl Saakashvili, est piratée par des hackers qui y ajoutent des photos comparant le chef de l'État à Adolf Hitler. L'accès de la Géorgie aux sites de la BBC et de CNN est également bloqué. Les Géorgiens tentent rapidement de répondre mais, à nouveau, l'origine des attaques est imprécise : les *botnets* responsables sont localisés en Russie mais également au Canada, en Turquie et... en Estonie [Clarke et Knake, p. 19]. Échouant à rétablir son système informatique gouvernemental, la Géorgie s'en remet à la société américaine Google qui transfère le site présidentiel sur un de ses serveurs en Californie.

8. L'article 5 du traité de Washington stipule : « Les parties conviennent qu'une attaque armée contre l'une ou plusieurs d'entre elles survenant en Europe ou en Amérique du Nord sera considérée comme une attaque dirigée contre toutes les parties, et en conséquence elles conviennent que, si une telle attaque se produit, chacune d'elles, dans l'exercice du droit de légitime défense, individuelle ou collective, reconnu par l'article 51 de la charte des Nations unies, assistera la partie ou les parties ainsi attaquées en prenant aussitôt, individuellement et d'accord avec les autres parties, telle action qu'elle jugera nécessaire, y compris l'emploi de la force armée, pour rétablir et assurer la sécurité dans la région de l'Atlantique nord. »

Hérodote, n° 152-153, La Découverte, 2e trimestre 2014.

À nouveau, le Kremlin nie toute implication dans ces actes perpétrés par des acteurs isolés et les relativise : des groupuscules de hackers nationalistes russes ont déjà commis des méfaits semblables sur les serveurs tchétchènes à la fin des années 1990 [Soldatov et Borogan, p. 230]. Néanmoins, les cyberattaques de 2008 se révèlent beaucoup plus efficaces pour une simple raison : leur concordance avec le rythme des manœuvres militaires russes. Le rapport du Pentagone sur la guerre informatique russo-géorgienne de 2008, *Overview by the US-CCU of the Cyber Campaign Against Georgia In August of 2008*, affirme que « les organisateurs des cyberattaques avaient une connaissance *a priori* des intentions militaires russes et bénéficiaient d'informations précises sur l'avancée des opérations avant que celles-ci soient menées » [Bumgarner et Borg, 2009].

Les cas estonien et géorgien influencent très certainement le groupe des experts présidé par Madeleine Albright en 2009-2010, qui est chargé des travaux préparatoires du nouveau Concept stratégique de l'Otan. La cyberdéfense y tient une part conséquente qui tranche avec l'aspect anecdotique de la déclaration de Prague. Dans le nouveau concept adopté lors du sommet de Lisbonne, un paragraphe entier lui est consacré :

> Les cyberattaques augmentent en fréquence, sont mieux organisées et causent des dommages plus coûteux aux administrations, aux entreprises, aux économies, voire aux réseaux de transport et d'approvisionnement ou autres infrastructures critiques ; elles risquent d'atteindre un seuil pouvant menacer la prospérité, la sécurité et la stabilité des États et de la zone euro-atlantique. Des forces armées et services de renseignement étrangers, la criminalité organisée, des groupes terroristes et/ou extrémistes sont autant de sources d'attaque possibles[9].

À l'issue du sommet de Lisbonne, le secrétaire général de l'Otan, Anders Fogh Rasmussen, décide de créer au sein du quartier général une nouvelle division chargée des « défis de sécurité émergents ». Au côté de thématiques stratégiques classiques telles que le terrorisme ou la prolifération d'armes de destruction massive, y figure la cyberdéfense.

Par ailleurs, les Alliés décident de réviser la politique de cyberdéfense (*Cyber Defense Policy*) formulée seulement deux ans auparavant. Il s'ensuit une séquence de multiples échanges entre les représentations nationales autour du mandat de l'Otan dans le cyberespace, la gouvernance au sein de l'organisation et les moyens requis. Après un semestre de négociations, le nouveau document est approuvé lors de la rencontre des ministres de la Défense de l'Alliance le 8 juin 2012. En substance, le texte ne fait que rappeler le périmètre minimal qui est octroyé à l'organisation : celle-ci doit avant tout défendre ses propres réseaux. Il est certes

9. <www.nato.int>

fait mention d'un besoin de « fournir assistance aux Alliés pour obtenir un niveau minimal de cyberdéfense et réduire les vulnérabilités des infrastructures critiques nationales » [NATO, 2011]. Mais, par souci de consensus, le document reste plus évasif sur l'étendue de cette assistance.

ENCADRÉ 1. SÉLECTION D'ORGANISATIONS DE L'OTAN S'OCCUPANT DE CYBERDÉFENSE

*** Siège de l'Otan : Division Défis de sécurité émergents**

La Division Défis de sécurité émergents s'occupe de l'éventail croissant des risques et des défis de sécurité non traditionnels, comme le terrorisme, la prolifération des armes de destruction massive, les questions nucléaires, les cyberattaques et l'insécurité énergétique.

*** Agence de services de systèmes d'information et de communications de l'Otan (NCSA)**

Elle est chargée de fournir des services techniques et opérationnels en matière de cybersécurité pour l'Otan et ses opérations, et elle supervise le NCIRC.

*** Bureau de consultation, contrôle et commandement de l'Otan (nc3)**

Organe directeur de l'Agence NC3A.

*** Agence de consultation, contrôle et commandement de l'Otan (NC3A)**

Elle est chargée d'identifier les aspects techniques et les besoins opérationnels des capacités de cyberdéfense de l'Otan, des acquisitions et de la mise en œuvre nécessaires à ces capacités. Elle a la responsabilité d'établir les nouveaux moyens de défense cybernétique de l'Otan.

*** Commandement allié Transformation (ACT)**

Adopte de nouveaux concepts opérationnels..., détermine leur viabilité et valeur, les fait aboutir par le biais du développement de doctrines, de la recherche scientifique, de l'expérimentation et du développement technologique. Il supervise le CCD-COE.

*** Centre d'excellence pour la cyberdéfense en coopération**

Il a pour but d'améliorer la capacité, la coopération et le partage d'information en matière de cyberdéfense à travers l'éducation, la recherche et le développement, les leçons apprises et la consultation.

La grande nouveauté est finalement l'institutionnalisation de la dimension informatique au sein du processus de planification de l'Otan que le texte consacre. Depuis lors, la cyberdéfense est devenue un sujet « routinier » des travaux du comité militaire de l'Alliance. Anecdote significative, les exercices

Hérodote, n° 152-153, La Découverte, 2e trimestre 2014.

de crise conduits par le quartier général incorporent désormais un scénario de cyberattaques.

Pour l'heure, le quartier général mène d'intenses consultations sur la possibilité de créer une capacité propre à l'Alliance qui puisse déployer en un temps rapide des moyens de cyberdéfense auprès d'un allié lorsque ce dernier demande assistance. Le projet défendu par le cabinet du secrétaire général Rasmussen s'inspire explicitement du modèle de gouvernance de l'Alliance en ce qui concerne les batteries de défense antimissile Patriot mises à disposition notamment en Turquie. Mais ici aussi, la faisabilité technique d'une telle initiative reste sujette à caution. « D'un point de vue tant politique qu'opérationnel, cette proposition ne pourra déboucher que sur une offre d'expertise et non de matériel : certains États n'accepteraient pas de transférer leurs technologies et la pertinence technique d'une telle opération n'est pas avérée », nous confie un cadre de la section cyberdéfense au quartier général[10].

Ainsi, alors qu'approche le prochain sommet des chefs d'État de l'Alliance à Newport (Royaume-Uni), l'Otan a institutionnalisé la problématique de cyberdéfense en créant de multiples entités au sein de ses structures civiles et militaires. Pour autant, de nombreuses inconnues – politiques, légales et techniques – demeurent inchangées.

L'Union européenne : la prévalence de la cybersécurité sur la cyberdéfense

Comme l'Otan, c'est à partir de l'année 2000, que l'Union européenne prend conscience de la nécessité de définir et de mettre en place une politique de cybersécurité pour protéger les systèmes d'information et les réseaux de ses institutions. À l'instar des États qui la composent et des autres organisations internationales, les activités politiques et économiques de l'Union reposent entièrement sur l'utilisation quotidienne de technologies de l'information et de la communication, et l'absence de politique de sécurité de ces infrastructures exposait l'UE à des risques importants de dysfonctionnement. Afin de prévenir ces risques et de garantir la continuité des activités de l'Union, une politique comprenant deux volets est élaborée : le premier vise à renforcer la sécurité des systèmes d'information et des réseaux de l'ensemble des institutions de l'UE, et le second doit permettre d'améliorer la cybersécurité de l'ensemble de l'Union, c'est-à-dire sur les réseaux et systèmes de ses États membres.

On peut ici noter un processus similaire d'institutionnalisation du sujet au sein de l'UE. L'instauration d'une telle politique s'appuie, d'une part, sur l'adoption de

10. Entretien téléphonique des auteurs avec un haut fonctionnaire de l'Otan, octobre 2013.

multiples directives européennes et, d'autre part, sur la création d'agences européennes spécifiquement dédiées à la cybersécurité. Les directives européennes adoptées dès la fin des années 1990 relatives aux technologies de l'information et de la communication (TIC) s'inscrivent dans l'esprit des décisions juridiques de l'UE : elles cherchent à préserver à la fois les libertés individuelles des citoyens européens en protégeant les données relatives à leur identité, tout en garantissant la poursuite et la pérennité des activités commerciales et économiques électroniques par une sécurisation des technologies œuvrant aux transactions de biens[11]. Par la suite, la recherche systématique de la sécurisation des TIC s'est élargie à l'ensemble du spectre couvert par leur utilisation, ouvrant ainsi la voie à la sécurité des infrastructures de communication et d'accès à l'information (réseaux publics tels Internet, réseaux de téléphonie mobile, etc.).

La première étape de l'amélioration de la cybersécurité passe par l'institutionnalisation de la protection des systèmes d'information et des réseaux des institutions de l'Union. Pour ce faire, la direction « Sécurité, sûreté et systèmes d'information et de communication » du Conseil de l'Europe, par sa sous-direction « Direction 5 – Systèmes d'information et de communication », développe les procédures et standards de sécurité garantissant la protection de l'information circulant sur les réseaux de l'UE. Chargée d'élaborer la politique de sûreté de l'information (*Information Assurance Policy*) des réseaux de l'UE, cette direction s'assure que la protection des informations classifiées est garantie. D'autre part, depuis septembre 2012, un *Computer Emergency Response Team* (CERT) UE a été créé ; il s'agit d'un CERT dédié aux institutions européennes, qui regroupe les experts de sécurité informatique des différents corps de l'Union (Commission, Parlement, Conseil, comités, etc.) et qui a vocation à terme à être le centre opérationnel en charge de la sécurité des systèmes d'information et réseaux de l'ensemble des institutions de l'UE. Cette première étape permet aux instances de l'Union européenne d'étendre leur politique de cybersécurité pour la tourner vers les États membres, de manière à améliorer globalement le niveau de cybersécurité en Europe.

Ainsi, l'European Union Agency for Network and Information Security (ENISA) est créée en 2004 par une réglementation du Parlement européen et du Conseil de l'Europe (Regulation (EC) No 460/2004), pour aider la Commission et les États membres à atteindre le niveau de sécurité des systèmes d'information requis par les directives adoptées jusqu'alors. Les textes juridiques adoptés par les institutions de l'UE n'ayant pas pour vocation d'imposer des standards et normes

11. Parmi ces mesures, on peut citer cette liste non-exhaustive : directive 1999/93/EC, directive 2000/31/EC, directive 2002/19/EC, directive 2002/20/EC, directive 2002/21/EC, directive 2002/22/EC, directive 2002/58/EC, Commission Decision 2002/627/EC.

Hérodote, n° 152-153, La Découverte, 2e trimestre 2014.

techniques, c'est l'ENISA qui a endossé ce rôle ; l'agence produit alors toute une littérature relative aux procédures de gestion du risque des systèmes d'information et réseaux, à la protection de l'identité et des données personnelles en ligne, à la protection des infrastructures critiques de l'information (CIIP) et de leur résilience, ou encore au fonctionnement et à la collaboration de l'activité des CERT internationaux.

En agissant à plusieurs niveaux – en soutien à l'élaboration de politiques publiques, en facilitant la collaboration entre les États membres et au-delà, ainsi qu'en contribuant activement à la collecte de renseignements permettant la préparation face aux attaques –, l'ENISA est devenue en quelques années une véritable plateforme européenne permettant l'échange et le partage d'informations relatives à la cybersécurité entre les États membres mais aussi avec le secteur privé et d'autres acteurs internationaux. L'agence travaille en effet avec les personnes en charge d'instaurer et de gérer la cybersécurité dans différentes institutions (du secteur public comme du secteur privé), pour s'assurer que les mesures mises en place sont efficaces, en accord avec les directives européennes, respectant les activités des institutions, tout en garantissant un niveau élevé de sécurité. Afin de garantir une cohérence dans la réponse nationale des États membres de l'UE, l'ENISA a encouragé et conseillé les gouvernements pour l'instauration de CERT nationaux, puis a instauré la tenue d'exercices de simulation d'attaques au niveau européen (*Pan-European Cybersecurity Exercises*), pour évaluer le niveau de collaboration et de coordination des capacités de cybersécurité au niveau européen.

Au mois de mai 2013, le Parlement européen et le Conseil de l'Europe renouvellent et élargissent le mandat de l'ENISA (Regulation (EU) No 526/2013), par lequel l'agence bénéficie d'un rôle accru dans l'élaboration de politiques et de législations européennes relatives à la cybersécurité, accentue ses travaux de recherche et développement pour améliorer les standards de sécurité des TIC, est l'acteur référent pour la coopération de l'UE avec les acteurs internationaux et, enfin, agit en étroite collaboration avec le European Cybercrime Center d'Europol (EC3) pour lutter contre la cybercriminalité au sein de l'UE.

L'EC3 vient effectivement compléter les activités de l'ENISA en se spécialisant dans la lutte contre la cybercriminalité qui affecte les activités économiques et qui va à l'encontre des valeurs défendues par l'UE (attaques informatiques contre le secteur bancaire ou activités pédopornographiques). Basé dans les locaux d'Europol, l'EC3 doit établir avec l'ENISA les moyens de collaborer avec les CERT nationaux et les institutions judiciaires nationales afin de faciliter les enquêtes judiciaires souvent internationales et complexes.

La création de ces deux agences symbolise l'accélération de la mise en place de mesures de sécurité et de protection des citoyens européens dans le cyberespace. Les institutions politiques de l'Union ont en effet pris conscience de l'importance

des TIC dans l'activité économique et sociale européenne et mondiale actuelle, et ont en conséquence intégré des stratégies idoines dans les politiques publiques de l'Union européenne.

C'est ainsi qu'en mars 2010 la Commission européenne lance la stratégie « Europe 2020 » qui, par diverses initiatives ayant trait à l'emploi, l'éducation, la recherche et l'innovation, les enjeux énergétiques et environnementaux, ou encore la lutte contre la pauvreté et l'exclusion sociale, entend relancer et préparer la croissance économique de l'UE en adaptant ses politiques aux défis à venir. Parmi ces initiatives, la stratégie numérique pour l'Europe (*Digital Agenda for Europe*) souligne le rôle moteur que les TIC peuvent jouer pour atteindre les objectifs déterminés dans la stratégie « Europe 2020 », et identifie les manières d'exploiter le potentiel économique et social offert par ces technologies, selon sept piliers définissant les axes de travail, eux-mêmes déclinés en une centaine de mesures à mettre en place.

La cyberstratégie de l'Union européenne publiée en février 2013, *Cybersecurity Strategy of the European Union. An Open, Safe, and Secure Cyberspace* (« Stratégie de cybersécurité de l'Union européenne : un cyberespace ouvert, sûr et sécurisé »), est ainsi le produit de cette stratégie numérique pour l'Europe ; elle répond à un besoin identifié dans le *Digital Agenda for Europe* de renforcer les efforts de collaboration initiés entre la Commission européenne et les États membres pour améliorer la cybersécurité, qui manquent encore pour l'instant de cohérence. La nouvelle stratégie européenne s'accompagne d'une proposition de directive (COM(2013) 48 *final*) visant à garantir un haut niveau commun de sécurité des systèmes d'information par l'amélioration de la sécurité sur Internet, les réseaux privés, et l'information vitale au fonctionnement des sociétés de l'UE. Cette directive veut ainsi contraindre les États membres à renforcer les mesures de sécurité, de résilience des infrastructures dans les secteurs jugés critiques (énergie, transports, administration publique, économie, etc.), ainsi qu'imposer l'adoption de procédures de gestion du risque et de signalisation d'incidents/d'attaques, ou encore renforcer les procédures de coopération entre États membres.

Dès lors, la stratégie de cybersécurité de l'Union européenne de 2013 se présente comme une synthèse des mesures adoptées jusque-là dans le domaine et qui seront poursuivies, auxquelles viennent s'ajouter de nouvelles ambitions résolument plus politiques. Ainsi, au regard des cinq axes prioritaires de la cyberstratégie de l'UE (« Garantir la "cyberrésilience", réduire drastiquement la cybercriminalité, développer une politique et des capacités de cyberdéfense dans le cadre des missions militaires de l'UE, développer un réseau de ressources technologiques et industrielles de cybersécurité pour l'UE, définir une stratégie internationale de cybersécurité défendant les valeurs de l'UE »), on constate que les deux premiers sont déjà fortement établis et bénéficient de moyens techniques

Hérodote, n° 152-153, La Découverte, 2e trimestre 2014.

et juridiques conséquents ; ils ne sont que la traduction des mesures prises depuis une quinzaine d'années en « stratégie ».

Les deux derniers axes, sur le développement de ressources technologiques et industrielles et sur la stratégie internationale de l'UE, s'inscrivent dans cette logique duale qui constitue les fondations de l'Union européenne : d'un côté garantir, protéger, favoriser l'économie et le commerce entre les États membres, tout en assurant la protection des libertés individuelles et des droits fondamentaux des citoyens européens. L'encouragement d'un développement de « technologies européennes » pour la cybersécurité ne s'inscrit ainsi pas tant dans une logique strictement sécuritaire, qui verrait dans les produits « hors UE » une menace potentielle pour la sécurité, que dans une démarche de relance économique et industrielle, en cohérence avec la stratégie Europe 2020.

Quant à la stratégie internationale de cybersécurité de l'UE qui veut défendre sur la scène internationale la vision de l'Union européenne de la protection des libertés individuelles fondamentales dans le cyberespace, elle s'inscrit dans la continuité de ses actions précédentes. D'aucuns pourraient ainsi y voir une tentative de relancer sous une autre forme les valeurs déjà défendues dans la convention de Budapest sur la cybercriminalité[12], signée en 2001 par de nombreux États mais jamais vraiment respectée. Ces deux démarches, résolument politiques, n'en restent pas moins des initiatives intéressantes par lesquelles l'UE semble vouloir se positionner comme acteur majeur de la cybersécurité sur la scène internationale.

Le dernier axe de cette stratégie concerne la définition du besoin relatif aux capacités de cyberdéfense nécessaires pour les missions militaires de l'UE, dans le cadre de la Politique de sécurité et de défense commune (CSDP). Cette question vient immédiatement poser la question de la redondance avec les activités et les capacités de cyberdéfense de l'Otan. La question est actuellement étudiée au sein de l'Agence européenne de défense (AED), qui devrait fournir des pistes à la fin 2014. Quoi qu'il en soit, les « capacités de cyberdéfense qui pourront être employées par l'UE dans le cadre de missions CSDP seront cohérentes avec les besoins opérationnels et ne devraient pas reproduire les capacités Otan existantes. Ce ne serait dans l'intérêt de personne », nous confiait un expert travaillant sur le programme de l'AED[13].

La stratégie de cybersécurité de l'UE, synthétisée dans le texte de février 2013, s'avère cohérente ; elle encourage la poursuite des efforts déployés depuis la fin

12. La convention dite de Budapest sur la cybercriminalité visait à harmoniser les procédures pénales internationales eu égard aux infractions criminelles dans ou par le cyberespace. Cependant, la nature de certaines infractions, telles que définies dans la convention, se heurtait à certaines Constitutions nationales, limitant ainsi son application et donc sa portée.

13. Entretien des auteurs avec un expert de l'Agence européenne de défense, octobre 2013.

du siècle dernier qui sont nécessaires à la protection des activités fondamentales de l'Union et définit des objectifs futurs en harmonie avec sa ligne politique directrice : la pérennité de l'activité économique au sein de l'UE entre les États membres, et la garantie des libertés fondamentales des citoyens européens. La stratégie de cybersécurité de l'UE s'inscrit ainsi dans une continuité nécessaire et pose des bases pour des objectifs dans la mesure de son mandat et de ses capacités. Les questions relatives à une activité de cyberdéfense de l'UE ne sont en effet pas mises excessivement en avant, l'Union étant consciente de sa position d'acteur mineur dans ce domaine.

Enfin, les objectifs politiques définis dans la stratégie devront être confrontés à la réalité des relations internationales pour tester leur viabilité. À ce titre, les révélations d'Edward Snowden sur les programmes de surveillance des services américains ciblant les systèmes et réseaux de ses alliés européens[14] ont choqué par leur ampleur, tant sur le plan quantitatif que qualitatif, et permettent de constater l'inefficacité actuelle des mesures de protection mises en place par l'UE comme par ses États membres. On peut craindre que, devant de telles révélations, les États soient tentés de se replier sur eux-mêmes pour garantir la sécurité de leurs réseaux, délaissant une solution commune qui paraît pour le moment bien futile.

Les limites de l'intergouvernementalité dans le cyberespace

Comme ce tour d'horizon le suggère, l'intérêt grandissant des politiques des deux rives de l'Atlantique pour la cyberdéfense n'est pas sans susciter de multiples problèmes au sein d'une organisation comme l'Otan ou l'UE. Au sein de l'Alliance atlantique, le premier écueil renvoie aux profondes divergences de vues qui existent entre alliés sur le sujet. Si le principe de défendre les réseaux propres de l'Alliance est agréé par les 28 États membres, l'idée d'un rôle accru et plus englobant de l'organisation dans le domaine est encore loin de susciter un consensus dans une organisation qui ne peut décider sans unanimité.

La plupart des personnes interrogées décrivent les consultations au sein du Conseil de l'Atlantique nord comme le reflet d'une profonde division entre, d'un côté, les petits États qui disposent de peu de ressources propres dans le domaine de la lutte informatique et qui, logiquement, verraient d'un bon œil la gestion de leur cyberdéfense par l'Otan ; et, de l'autre, les quelques États (États-Unis,

14. Les révélations sur le programme de surveillance « Prism » ont été dévoilées par le quotidien britannique *The Guardian* en juillet 2013, puis ont été traduites et reprises dans une série d'articles par le quotidien *Le Monde*.

Hérodote, n° 152-153, La Découverte, 2e trimestre 2014.

Royaume-Uni, France, Allemagne) qui ont massivement investi dans le domaine, ont produit un vaste corpus doctrinal en matière de lutte informatique et ont parfois même constitué des Cyber Commandements. À ce titre, ces derniers ne souhaitent pas voir leur souveraineté s'effriter en raison d'une mutualisation de leurs ressources avec les autres alliés.

Outre la question de la souveraineté, les Alliés ne sont pas non plus en accord sur la problématique des capacités offensives dans le domaine. À nouveau, si la défense des réseaux est un sujet de consensus, la mise en œuvre d'une posture offensive telle que revendiquée par certains pays de l'Alliance mettent certains des membres dans l'embarras, notamment vis-à-vis du relatif flou juridique qui entoure la thématique. En 2010, la proposition du secrétaire à la Défense adjoint William Lynn d'ériger un groupe de planification de cyberdéfense au sein de l'Otan sur le modèle du groupe de planification nucléaire a ainsi soulevé une polémique quant au message politique qu'elle adressait. L'idée de Lynn avait le mérite de hausser le niveau de prise en charge de la problématique cyber à celui des décideurs politiques mais par là même elle cristallisait tous les contentieux doctrinaux, légaux et financiers que le dossier suscitait entre Alliés.

Mais, au-delà de l'éventualité d'une convergence de vues entre alliés, une autre inconnue est celle de la capacité réelle de l'Otan à agir dans le cyberespace. « Il y a un véritable décalage entre, d'un côté, les décideurs politiques qui sans maîtriser la dimension technique du sujet affirment "nous devons faire quelque chose !" et, de l'autre, la réalité qui est que l'Otan n'a pas un rôle évident hormis sur ses propres réseaux[15]. » Alors que le cyberespace est majoritairement contrôlé par des compagnies privées, l'Otan n'a que peu de prise sur ces acteurs. Il existe certes un groupe consultatif sur les relations Otan-Industrie qui peut identifier les segments de coopération entre l'Alliance et le secteur privé mais cela reste un domaine modeste dans lequel l'organisation internationale ne dispose pas, contrairement à l'Union européenne, de moyens contraignants qui puissent être mobilisés vis-à-vis des entreprises.

C'est précisément cet aspect que l'UE entend développer dans sa politique de cybersécurité. Bien que son intention première dans le domaine soit de garantir la sécurité des infrastructures permettant les échanges commerciaux de biens et de services entre les États membres, l'UE n'est pas sans savoir que l'amélioration substantielle de la sécurité de ces infrastructures servira à l'amélioration générale de la cybersécurité au sein des États membres. Or, dans le domaine des TIC, la grande majorité des infrastructures d'importance vitale sont la propriété du secteur privé. Ainsi, en adoptant des mesures successives instaurant cette garantie de

15. Entretien téléphonique des auteurs avec un haut fonctionnaire de l'Otan, octobre 2013.

sécurité, l'UE contribue dans une certaine mesure à réduire les vulnérabilités des infrastructures numériques.

L'Union européenne n'a toutefois qu'un rôle limité dans la construction de la cybersécurité, et cantonne ses mesures aux activités liées au secteur économique et commercial, dans le respect des libertés individuelles fondamentales qu'elle entend défendre dans le cyberespace (comme le rappelle la stratégie de 2013).

Les enjeux de souveraineté, qui inhibent les actions communes de cyberdéfense au sein de l'Otan, sont autant d'obstacles à l'adoption de mesures de cybersécurité plus développées au sein de l'UE. Il apparaît au terme de nos recherches que les États membres de l'Union qui ont massivement investi dans ce domaine ne céderont pas plus de terrain sur cette question au sein de l'UE qu'au sein de l'Otan ; en conséquence, les mesures de cybersécurité actuelles reposent majoritairement sur la coopération volontaire par laquelle les centres de cybersécurité nationaux, mais également ceux du secteur privé échangent et partagent des informations selon leurs besoins et leur bon vouloir. Les agences de l'Union européenne (l'ENISA et le CERT-EU) n'ont ainsi aucun pouvoir de contrainte, et ne peuvent que proposer des recommandations et des conseils relatifs aux bonnes pratiques dans le domaine.

Ainsi, la politique de cybersécurité de l'Union européenne s'inscrit dans la continuité de ses activités premières, et correspond principalement à la recherche de protection et de sécurisation optimale de ses outils de travail. L'UE cherche bien évidemment à développer cette politique au-delà de ces prérogatives, en élargissant les domaines au sein desquels l'Union pourrait avoir un rôle à jouer pour accroître la cybersécurité au niveau régional voire mondial, mais, en raison du caractère particulièrement sensible de ces questions, les États opposent la notion de souveraineté à toute velléité d'extension ou de mise en commun des capacités. C'est d'autant plus frappant dans les domaines militaires et du renseignement, où l'UE n'aura *a fortiori* qu'un rôle similaire à celui qu'elle joue actuellement, c'est-à-dire cantonné à la protection des réseaux et outils de communication de la chaîne de commandement militaires de l'Union européenne (EU OPS-WAN par exemple).

Conclusion

En conclusion, il ressort de notre enquête un constat en demi-teinte. L'Otan et l'UE ont indéniablement adapté leurs administrations aux problématiques liées au cyberespace comme en témoignent la pléthore de directives, de stratégies et autres documents produits par les deux organisations mais aussi la création en leur sein de nouvelles structures dédiées. Pour autant, si la politisation du sujet a engendré une inflation bureaucratique, elle n'a pas résolu certaines questions essentielles. Force est de constater, au travers de notre étude comparée, qu'une certaine

Hérodote, n° 152-153, La Découverte, 2e trimestre 2014.

confusion règne sur les rôles de l'Otan et de l'UE dans le domaine, notamment en ce qui concerne la sphère militaire. Il est bien difficile de voir émerger des éléments de subsidiarité ou de complémentarité des travaux de chacun. Comme sur de nombreux autres sujets internationaux, les deux organisations ont conçu et développé leurs politiques parallèlement et non conjointement. Mais, *in fine*, c'est surtout la question de la souveraineté nationale, en tant que ligne rouge de la coopération intergouvernementale, qui a freiné et devrait continuer à freiner les efforts tant de l'Otan que de l'UE. Avec les retombées de l'affaire Snowden, cette dialectique entre intergouvernementalité et souveraineté nationale n'est probablement pas près d'être dépassée dans le cyberespace.

Bibliographie

BENITEZ J. (2013), « EU invites NATO to boost cyber cooperation », *Atlantic Council*, mai.

BUMGARNER J. et BORG S. (2009), *Overview by the US-CCU of the Cyber Campaign Against Georgia In August of 2008*, US-CCU Special Report, US Department of Defense.

CLARKE R. et KNAKE R. (2010), *Cyberwar. The Next Threat to National Security and What To Do About It*, Harper Collins, New York.

EUROPEAN DEFENSE AGENCY (2013), « EDA study identifies cooperation prospects in cyber defence », communiqué de presse, mai.

GRANT R. (2007), *Victory in Cyberspace*, Air Force Association, Washington.

HEALEY J. et VAN BOCHOVEN L. (2012), « NATO's cyber capabilities : yesterday, today, and tomorrow », *Atlantic Council*, Issue Brief, février.

HEGENBART C. (2013), « NATO's cyber past, present and future », *Vox Collegii*, vol. VII, juillet 2013, p. 18-23.

IHEDN (2012), « Vers une cyberstratégie européenne ? », 4e séminaire IHEDN de Bruxelles, 28 juin.

JOUBERT V. (2012), « Five years after Estonia's cyber attacks : lessons learned for NATO ? », NATO Defense College, Research Paper n° 76, mai.

MINISTÈRE DE LA DÉFENSE (2011), « Étude sur la cyberdéfense et la cybersécurité au sein des institutions européennes », Esteral Consulting pour la délégation aux Affaires stratégiques, Paris, novembre.

NATO PUBLIC DIPLOMACY DIVISION (2011), *Defending the Networks. The NATO Policy on Cyber Defence*, Bruxelles.

SOLDATOV A. et BOROGAN I. (2010), « The new nobility. The restoration of Russia's security state and the enduring legacy of the KGB », *Public Affairs,* New York.

MORIN-DESAILLY C. (2013), « L'Union européenne, colonie du monde numérique ? », rapport d'information fait au nom de la commission des Affaires européennes, n° 443, Sénat, mars.

PARLEMENT EUROPÉEN (2013), « Cyberattaques : le Parlement adopte des sanctions communes plus strictes », communiqué de presse, juillet.

ROMAN J. (2013), « ENISA's enhanced cyber security role », *GovInfo Security*, juillet.