Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Verwaltungspraxis der Bundesbehörden VPB
Jurisprudence des autorités administratives de la Confédération JAAC
Giurisprudenza delle autorità amministrative della Confederazione GAAC

JAAC 3/2009 du 2 septembre 2009

2009.10b (p. 178-214)

Avis de droit sur les bases légales des opérations dans les réseaux informatiques par les services du DDPS

DFJP, Office fédéral de la justice et DFAE, Direction du droit international public

Avis de droit du 10 mars 2009

Mots clés: Opérations dans les réseaux informatiques, service de renseignements, CND, CNE, CNA, sphère privée, ius ad bellum, ius contra bellum, cybercriminalié**.**

Stichwörter: Computernetzwerkoperationen, Nachrichtendienst, CND, CNE, CNA, Privatsphäre, ius ad bellum, ius contra bellum, Cyber-Kriminalität.

Termini chiave: Operazioni nelle reti informatiche, servizio informazioni, CND, CNE, CNA, sfera privata, ius ad bellum, ius contra bellum, cibercriminalità.

Regeste:
Les bases légales actuelles sont suffisantes pour justifier les mesures non-agressives de défense de réseaux informatiques (Computer Network Defense, CND). Les mesures d'exploitation de réseaux informatiques (Computer Network Exploitation, CNE) et les attaques de réseaux informatiques (Computer Network Attack, CNA) sont aujourd'hui possibles dans le cadre du service actif. Comme une CNA ne peut être effectuée que dans le cadre du service actif,une base légale expresse n'est nécessaire. Pour procéder à des CNE, une base légale formelle est toutefois requise. La base légale sur laquelle se fonde actuellement le service de renseignements (art. 99 LAAM) ne permet pas la recherche des informations par le biais de CNE

Regeste:
Die heutigen Rechtsgrundlagen genügen für nicht-aggressive Computer Network Defense (CND). Computer Network Exploitation (CNE) und Computer Network Attack (CNA) sind heute nur im Aktivdienst möglich. Für die anderen Einsatzarten bestehen keine gesetzlichen Grundlagen. Da CNA nur im Aktivdienst durchgeführt werden soll, ist keine formell-gesetzliche Grundlage notwendig. Will man CNE betreiben, bedingt dies eine formell-gesetzliche Grundlage. Die bestehende Rechtsgrundlage für den Nachrichtendienst (Art. 99 MG) erlaubt keine Informationsbeschaffung mittels CNE

Regesto:
Le basi legali attuali sono sufficienti per giustificare le misure non aggressive di difesa delle reti informatiche (Computer Network Defense, CND). Oggi le misure di gestione delle reti informatiche (Computer Network Exploitation, CNE) e gli attacchi alle reti informatiche (Computer Network Attack, CNA) sono possibili solo nell'ambito di un servizio attivo. Siccome gli CNA possono essere effettuati solo nell'ambito del servizio attivo, non è necessaria una base legale formale. Per gestire una CNE, è indispensabile una base legale formale. La base legale attuale per il servizio informazioni (art. 99 LM) non permette la ricerca di informazioni mediante la CNE.

Base juridique:
Art. 5, art. 13, art. 16, art. 36, art. 58 al. 2; art. 173 al. 1, art. 185 al. 4 Cst. (RS 101);
Art. 8, art. 10, art. 13 de la Convention du 4 novembre 1950 de sauvegarde des droits de l'homme et des libertés fondamentales (CEDH; RS 0.101);

Loi du 21 mars 1997 sur l'organisation du gouvernement et de l'administration (LOGA; RS 172.010);
Ordonnance du 26 septembre 2003 sur l'informatique et la télécommunication dans l'administration fédérale (Ordonnance sur l'informatique dans l'administration fédérale, OIAF; RS 172.010.58);
Ordonnance du 7 mars 2003 sur l'organisation du Département fédéral de la défense, de la protection de la population et des sports (Org-DDPS; RS 172.214.1);
Art. 1, art. 65, art. 66, art. 66b, art. 70, art. 99, art. 100 al. 1 lit. b de la loi fédérale du 3 février 1995 sur l'armée et l'administration militaire (LAAM; RS 510.10);
Loi fédérale du 21 mars 1997 instituant des mesures visant au maintien de la sûreté intérieure (LMSI; RS 120);
Ordonnance du 10 juin 1996 concernant la mobilisation (OMob; RS 519.1);
Ordonnance du 2 décembre 2005 sur le personnel affecté à la promotion de la paix, au renforcement des droits de l'homme et à l'aide humanitaire (OPers-PDHH; RS 172.220.111.9);
Ordonnance du 26 février 1997 sur le service de promotion de la paix (RS 172.220.111.91);
Ordonnance du 3 septembre 1997 sur le recours à la troupe pour assurer la protection de personnes et de biens (OPPB; RS 513.73);
Ordonnance du 3 mai 2006 concernant l'engagement de la troupe pour la protection de personnes et de biens à l'étranger (OPPBE; RS 519.4);
Ordonnance du 8 décembre 1997 réglant l'engagement de moyens militaires dans le cadre d'activités civiles et d'activités hors du service (OEMC; RS 510.212);
Ordonnance du 29 octobre 2003 sur l'aide militaire en cas de catastrophe dans le pays (OAMC; RS 510.213);
Ordonnance du 15 octobre 2003 sur la guerre électronique (OGE; RS 510.292);
Ordonnance du 15 septembre 1997 concernant l'informatique au Département fédéral de la défense, de la protection de la population et des sports (Ordonnance INF DDPS; RS 510.211.2).

Rechtliche Grundlagen:
Art. 5, Art. 13, Art. 16, Art. 36, Art. 58 Abs. 2; Art. 173 Abs. 1, Art. 185 Abs. 4 BV (SR 101);
Art. 8, Art. 10, Art. 13 Konvention vom 4. November 1950 zum Schutze der Menschenrechte und Grundfreiheiten (EMRK; SR 0.101);
Regierungs- und Verwaltungsorganisationsgesetz vom 21. März 1997 (RVOG; SR 172.010);
Verordnung vom 26. September 2003 über die Informatik und Telekommunikation in der Bundesverwaltung (Bundesinformatikverordnung, BinfV; SR 172.010.58);
Organisationsverordnung vom 7. März 2003 für das Eidgenössische Departement für Verteidigung, Bevölkerungsschutz und Sport (OV-VBS; SR 172.214.1);
Art. 1, Art. 65, Art. 66, Art. 66b, Art. 70, Art. 99, Art. 100 Abs. 1 lit. b Bundesgesetz vom 3. Februar 1995 über die Armee und die Militärverwaltung (Militärgesetz, MG; SR 510.10);
Bundesgesetz vom 21. März 1997 über Massnahmen zur Wahrung der inneren Sicherheit (BWIS ; SR 120);
Verordnung vom 10. Juni 1996 über die Mobilmachung (VMobSR; 519.1);
Verordnung vom 2. Dezember 2005 über das Personal für die Friedensförderung, die Stärkung der Menschenrechte und die humanitäre Hilfe (PVFMH; SR 172.220.111.9);
Departementsverordnung vom 26. Februar 1997 über den Friedensförderungsdienst (SR 172.220.111.91);
Verordnung vom 3. September 1997 über den Truppeneinsatz zum Schutz von Personen und Sachen (VSPS; SR 513.73);
Verordnung vom 3. Mai 2006 über den Truppeneinsatz zum Schutz von Personen und Sachen im Ausland (VSPA; SR 519.4);
Verordnung vom 8. Dezember 1997 über den Einsatz militärischer Mittel für zivile und ausserdienstliche Tätigkeiten (VEMZ; SR 510.212);
Verordnung vom 29. Oktober 2003 über die militärische Katastrophenhilfe im Inland (VmKI; SR 510.213);
Verordnung vom 15. Oktober 2003 über die elektronische Kriegführung (VEKF; SR 510.292);
Verordnung vom 15. September 1997 über die Informatik im Eidgenössischen Departement für Verteidigung, Bevölkerungsschutz und Sport (Informatikverordnung VBS; SR 510.211.2).

Basi legali:
Art. 5, art. 13, art. 16, art. 36, art. 58 al. 2; art. 173 al. 1, art. 185 al. 4 Cst. (RS 101);
Art. 8, art. 10, art. 13 de la Convention du 4 novembre 1950 de sauvegarde des droits de l'homme et des libertés fondamentales (CEDH; RS 0.101);
Loi du 21 mars 1997 sur l'organisation du gouvernement et de l'administration (LOGA; RS 172.010);
Ordonnance du 26 septembre 2003 sur l'informatique et la télécommunication dans l'administration fédérale (Ordonnance sur l'informatique dans l'administration fédérale, OIAF; RS 172.010.58);
Ordonnance du 7 mars 2003 sur l'organisation du Département fédéral de la défense, de la protection de la population et des sports (Org-DDPS; RS 172.214.1);

Art. 1, art. 65, art. 66, art. 66b, art. 70, art. 99, art. 100 al. 1 lit. b de la loi fédérale du 3 février 1995 sur l'armée et l'administration militaire (LAAM; RS 510.10);
Loi fédérale du 21 mars 1997 instituant des mesures visant au maintien de la sûreté intérieure (LMSI; RS 120);
Ordonnance du 10 juin 1996 concernant la mobilisation (OMob; RS 519.1);
Ordonnance du 2 décembre 2005 sur le personnel affecté à la promotion de la paix, au renforcement des droits de l'homme et à l'aide humanitaire (OPers-PDHH; RS 172.220.111.9);
Ordonnance du 26 février 1997 sur le service de promotion de la paix (RS 172.220.111.91);
Ordonnance du 3 septembre 1997 sur le recours à la troupe pour assurer la protection de personnes et de biens (OPPB; RS 513.73);
Ordonnance du 3 mai 2006 concernant l'engagement de la troupe pour la protection de personnes et de biens à l'étranger (OPPBE; RS 519.4);
Ordonnance du 8 décembre 1997 réglant l'engagement de moyens militaires dans le cadre d'activités civiles et d'activités hors du service (OEMC; RS 510.212);
Ordonnance du 29 octobre 2003 sur l'aide militaire en cas de catastrophe dans le pays (OAMC; RS 510.213);
Ordonnance du 15 octobre 2003 sur la guerre électronique (OGE; RS 510.292);
Ordonnance du 15 septembre 1997 concernant l'informatique au Département fédéral de la défense, de la protection de la population et des sports (Ordonnance INF DDPS; RS 510.211.2).

Contenue

Glossaire des abréviations les plus importantes

CNA	computer network attack (attaque de réseaux informatiques)
CND	computer network defense (défense de réseaux informatiques)
CNE	computer network exploitation (exploitation de réseaux informatiques)
CNO	computer network operations (opérations dans les réseaux informatiques)
SAP	Service d'analyse et de prévention (DDPS)
EW	Electronic Warfare (combat électronique)
BAC	Base d'aide au commandement
InfoOps	Opérations d'information
MILDEC	Military Deception (déception militaire)
Cond info op	conduite de l'information opérationnelle
OPSEC	Operations Security (sécurité des informations)
PSYOPS	Psychological Operations (opérations psychologiques)

La Délégation des Commissions de gestion (DelCdG) a posé les questions suivantes à l'Office fédéral de la justice et à la Direction du droit international public qui y répondent par un avis de droit commun:

1. *Les bases légales existantes sont-elles suffisantes pour autoriser la défense de réseaux informatiques (CND)?*
2. *Quelles sont les bases légales qui autorisent les services du DDPS à procéder à l'exploitation de réseaux informatiques (CNE) et à l'attaque de réseaux informatiques (CNA)? Dans le cadre de quels genres d'engagements de l'armée peut-on faire appel à des CNE et à des CNA?*
3. *Qu'en est-il des bases légales existantes applicables au service de renseignements (art. 99 LAAM) par rapport à celles qui pourraient régir les InfoOps de l'armée, en particulier la recherche des informations par le biais de CNE?*
4. *Quelles conséquences aurait l'adoption du nouvel art. 18m LMSI (perquisition secrète d'un système informatique) sur les opérations de CNE et de CNA ?*

Le document s'articule comme suit: après un exposé approfondi de la situation initiale, l'analyse porte sur la question de savoir dans quelle mesure des bases légales sont nécessaires pour procéder à des opérations dans les réseaux informatiques (CNO). Les questions juridiques se posent avant tout au sujet des CNE (voir ch. 2.2). Un exposé détaillant les conditions de droit international public applicables aux CNO conclut l'analyse. Ce point est surtout déterminant pour les CNA (voir ch. 3).

1. Contexte

1.1. Définitions

InfoOps, c'est-à-dire les informations d'opérations. Elles englobent toutes les actions de la cond info op, EW, CNO, MILDEC et OPSEC, ayant pour but d'influencer le processus de prise de décision d'un adversaire, de perturber ce processus, de l'altérer ou de l'exploiter, tout en protégeant son propre processus[1].

Selon la définition proposée par le DDPS pour la Suisse, les CNO désignent toutes les actions militaires ci-après, opérées dans un réseau informatique ou à l'aide d'un tel réseau: CND: mesures prises en vue de contrôler et de défendre ses propres équipements informatiques; CNE: mesures permettant d'accéder à des données contenues dans des équipements informatiques appartenant à autrui; CNA: mesures par lesquelles il est porté atteinte à l'intégrité et à l'accessibilité de réseaux informatiques et aux données qu'ils contiennent.

Les trois catégories principales de CNO sont décrites ci-après. Le graphique 1 (CNO) figurant en annexe montre la difficulté qu'il y a à opérer une séparation distincte entre ces trois catégories et les zones floues qui en résultent. Il peut servir du moins à illustrer à quel point les limites entre la guerre et la paix dans le contexte des CNE et des CNA sont confuses[2].

Dans le présent avis, nous examinerons les zones floues à l'aune des bases légales de droit interne en considérant à chaque fois le degré le plus élevé de CNE et de

[1] Cond info op: conduite de l'information opérationnelle (dans le langage international, on parle de PSYOPS, Psychological Operations); EW: Electronic Warfare; CNO: Computer Network Operations; MILDEC: Military Deception; OPSEC: Operations Security.

[2] Pour plus de détails, voir ch. 3.2.1.

CNA. Ainsi les contre-attaques défensives opérées dans le cadre de CND tombent déjà, par exemple, dans la catégorie des CNA.

Par CND, on entend les mesures préventives destinées à protéger les réseaux informatiques militaires du front (p. ex. les systèmes d'armes) et leur contenu, la détection préalable d'éventuelles attaques et la mise sur pied de contre-mesures en cas d'attaque. La CND outrepasse la limite de la pure défense en cas de recours effectif à des contre-mesures ou à une contre-attaque (CNA); il en va de même lorsque la récolte active d'informations intervient dans la sphère de l'agresseur (CNE)[3]. En tant qu'action de pure défense en cas de danger, la CND, en ce sens, ne se distingue pas véritablement des mesures de sécurité informatique telle qu'elles se pratiquent dans les domaines privé et public. La CND est aujourd'hui déjà utilisée par la Base d'aide au commandement (BAC)[4].

Les CNE constituent des actions qui permettent, par l'utilisation de réseaux informatiques, de récolter des informations depuis ou dans des ordinateurs ou réseaux informatiques appartenant à des adversaires, sans modifier le contenu et l'état du système. On assimilera dans cet avis les CND ayant pour but la récolte active et avérée d'informations sur les ressources de l'adversaire à des CNE[5]. Selon les renseignements fournis par le DDPS, aucun service en Suisse ne recourt actuellement aux CNE. Compte tenu de leurs spécificités, il s'agit d'activités propres à des services de renseignements menées principalement contre d'autres armées ou d'autres Etats.

Pour donner un exemple concret de recours aux CNE, on peut renvoyer au programme Skype. Skype permet de converser gratuitement avec d'autres usagers de Skype par internet. S'agissant de messages cryptés, ceux-ci ne pourraient être écoutés, en l'état actuel des connaissances, que par l'introduction d'un cheval de Troie dans le système visé.

On désigne par CNA les actions qui, par l'utilisation de réseaux informatiques, ont pour but d'entraver, d'empêcher ou de ralentir l'accès à des informations contenues dans des ordinateurs ou dans des réseaux informatiques, ou de détruire les informations relatives à ces réseaux informatiques ou à ces ordinateurs. Le présent avis compte aussi les CNE agressives ainsi que les contre-attaques défensives au nombre des CNA[6]. Selon les renseignements fournis par le DDPS, aucun service en Suisse ne recourt actuellement aux CNA.

1.2. Genres d'engagements de l'armée

En vertu de l'art. 65 LAAM, l'armée est engagée dans le cadre du service de promotion de la paix, du service d'appui et du service actif[7]. Ces trois genres d'engagements sont brièvement exposés ci-après.

Les engagements pour la promotion de la paix peuvent être ordonnés sur la base d'un mandat de l'ONU ou de l'OSCE (art. 66, al. 1, LAAM)[8]. Le service de promotion de la paix est accompli par des personnes ou des troupes suisses spécialement formées à cet effet (art. 66, al. 2, LAAM). Le Conseil fédéral est compétent pour ordon-

[3] Il s'agit des zones figurées en gris dans le graphique 1 (CNO) en annexe – celles-ci doivent être prises en compte pour chaque degré consécutif le plus élevé de CNE et de CNA.

[4] Cf. l'exposé du 8 mars 2008 du Div. K. Nydegger, chef de la Base d'aide au commandement BAC, à l'occasion de l'assemblée annuelle de la Société Suisse des Officiers Aide au Commandement, p.18 ss.

[5] Voir le graphique 1 (CNO) en annexe et le principe exposé sous n. 3.

[6] Voir le graphique 1 (CNO) en annexe et le principe exposé sous n. 3.

[7] Cf. à ce sujet PATRICK SUTTER, Recht der militärischen Operationen, in: Sécurité & Droit 1 (2008) 19.

[8] Voir aussi l'ordonnance du Conseil fédéral du 2 décembre 2005 sur le personnel affecté à la promotion de la paix, au renforcement des droits de l'homme et à l'aide humanitaire (OPers-PDHH), RS 172.220.111.9, ainsi que l'ordonnance du Département militaire fédéral du 26 février 1997 sur le service de promotion de la paix, RS 172.221.104.41.

ner de tels engagements. Ils sont toutefois soumis à l'approbation de l'Assemblée fédérale lorsqu'ils sont armés, que l'effectif dépasse 100 militaires ou qu'ils durent plus de trois semaines (art. 66*b* LAAM).

Conformément à l'art. 1, al. 3, LAAM, l'armée soutient les autorités civiles lorsque leurs moyens ne suffisent plus pour faire face aux menaces graves contre la sécurité intérieure et pour maîtriser d'autres situations extraordinaires, en particulier en cas de catastrophe dans le pays ou à l'étranger (service d'appui)[9]. L'art. 58, al. 2, Cst. limite cependant l'assistance de l'armée aux autorités civiles appelées à faire face à une grave menace pesant sur la sécurité intérieure ou à d'autres situations d'exception. L'art. 1, al. 3, LAAM doit s'apprécier à la lumière des conditions posées par la Constitution en ce qui concerne la mission attribuée à l'armée de soutenir les autorités civiles lorsque leurs moyens ne suffisent plus pour faire face aux menaces graves contre la sécurité intérieure et/ou pour maîtriser d'autres situations extraordinaires, en particulier en cas de catastrophe dans le pays ou à l'étranger. Il n'y a ainsi que les autorités fédérales chargées de faire face aux menaces graves contre la sécurité intérieure et de maîtriser d'autres situations extraordinaires qui sont visées par la notion d'autorités civiles au sens de l'art. 58, al. 2, Cst.

Il faut au surplus garder à l'esprit que l'engagement de l'armée repose toujours sur le principe de la subsidiarité conformément à l'art. 58 Cst.[10]. Les missions de longue durée doivent être assurées par les forces de police sans recours à l'armée[11].

Sont compétents le Conseil fédéral et, en cas de catastrophe en Suisse, le DDPS pour la mise sur pied du service d'appui. L'Assemblée fédérale doit cependant approuver l'engagement du service d'appui si celui-ci dure plus de trois semaines (art. 70 LAAM).

Le service actif est accompli pour défendre la Suisse et sa population (service de défense nationale), soutenir les autorités civiles en cas de menaces graves contre la sécurité intérieure (service d'ordre), et améliorer le niveau de l'instruction de l'armée en cas d'accroissement de la menace[12].

En vertu de l'art. 173, al. 1, Cst., l'Assemblée fédérale est compétente pour ordonner le service actif; cette compétence n'est attribuée au Conseil fédéral que dans les cas d'urgence et celui-ci doit convoquer l'Assemblée fédérale s'il met sur pied plus de 4'000 militaires ou si cet engagement doit durer plus de trois semaines (art. 185, al. 4, Cst.).

1.3. Organisation

Tout type de CNO n'entre pas en ligne de compte pour tous les genres d'engagements décrits ci-dessus. A ce titre, nous sommes également d'avis que des CNO ne peuvent être effectuées dans le cadre d'un service d'instruction (art. 41 ss LAAM) que si une base légale spécifique les autorise expressément.

Aucun des genres d'engagements prévus à l'art. 65 LAAM n'est nécessaire pour effectuer des opérations de CND, car sinon celles-ci ne pourraient pas être exécutées. En effet, le but des CND est de garantir le fonctionnement des systèmes d'armement

[9] Cf. à ce sujet l'ordonnance du 3 septembre 1997 sur le recours à la troupe pour assurer la protection de personnes et de biens (OPPB), RS 513.73; l'ordonnance du 3 mai 2006 sur le recours à la troupe pour la protection de personnes et de biens à l'étranger (OPPBE), RS 519.4; l'ordonnance du 8 décembre 1997 réglant l'engagement de moyens militaires dans le cadre d'activités civiles et d'activités hors du service (OEMC), RS 510.212; l'ordonnance du 29 octobre 2003 sur l'aide militaire en cas de catastrophe dans le pays (OAMC), RS 510.213.

[10] HANSJÖRG MEYER in: Die Schweizerische Bundesverfassung. Kommentar, 2ème édition, Zurich/St-Gall 2008 (Commentaire St-Gallois), ART. 58, RZ. 16 *in fine*.

[11] SUTTER (n. 7), 28.

[12] Art. 76 LAAM. Voir aussi l'ordonnance du 10 juin 1996 concernant la mobilisation (OMob), RS 519.1.

et des réseaux informatiques de l'armée en continu; il s'agit d'un outil indispensable faisant partie intégrante du système.

Sous réserve de l'existence d'une base légale, aucun des trois genres d'engagements ne peut actuellement donner lieu à la mise en œuvre de CNE; il n'est pas à exclure en revanche que l'engagement dans le cadre du service de promotion de la paix et du service d'appui donne lieu à des mesures ressortissant à la CND et à la CNE.

En ce qui concerne les CNA et les zones floues qui s'y rattachent, seul le service actif – et dans tous les cas dès que l'on a franchi le seuil de l'attaque armée[13] - peut en justifier le recours; dans ce type d'engagement, les trois catégories de CNO apparaissent en principe comme licites[14]; voir à ce sujet le graphique 2 (engagement de l'armée pour procéder à des CNA) en annexe.

En cas de conflit armé, ce sont les règles du droit international public (*ius ad bellum*, droit de la neutralité, *ius in bello*)[15] qui s'appliquent à tous les types de CNO.

En dehors du service actif, il n'existe aucune base légale légitimant le recours à des CNA.

Nous sommes d'avis que les CNA ne devraient trouver application qu'en cas de guerre – menée en l'occurrence par l'armée -, ce qui rend superflue la création d'une base légale applicable en temps de paix. Dans ces conditions, il appartient à la BAC de développer des capacités à cet effet.

La BAC devrait désormais (pouvoir) assurer les trois catégories de CNO, à savoir les CND, les CNE et les CNA.

La BAC[16] a pour mission, dans le cadre de ses attributions générales confiées par l'armée, d'assurer le fonctionnement de ses systèmes de commandement informatisés et électroniques[17]. Sur la base d'un mandat approprié (limité dans le temps), l'armée peut implanter dans le cadre de ses différents genres d'engagement en Suisse et à l'étranger, des systèmes de renseignements et de brouillage. La BAC est chargée de se procurer (avec armasuisse) et d'installer les systèmes adéquats (tant sur le plan tactique qu'opérationnel) au sein des troupes.

Aujourd'hui déjà, les agents de la FUB assurent l'exploration radio en permanence[18]. Ils captent les rayonnements électromagnétiques militaires et civils émanant d'antennes, de satellites et d'autres installations analogues depuis l'étranger. S'ils le souhaitent, ils peuvent transformer ces rayonnements en informations isolées identifiables et lisibles. L'instrument le plus important utilisé actuellement à cet effet est le système ONYX. Celui-ci vise principalement les communications civiles par satellite et est utilisé dans le cadre de l'exploration radio permanente[19]. Selon l'usage cou-

[13] Pour plus de détails voir ch. 3.2.2.1. ss.

[14] Cf. l'art. 36, al. 1, Cst, qui autorise la restriction de droits fondamentaux sans base légale en cas de danger sérieux, direct et imminent. Voir RAINER J. SCHWEIZER, in: Commentaire St-Gallois (Rz. 10), art. 36, Rz. 17 et les renvois y relatifs.

[15] Pour plus de détails, voir ch. 3.

[16] La BAC est le résultat de la fusion du groupe d'aide au commandement (gr aide cdmt) et de la Direction de l'informatique du DDPS (dir inf DDPS). Office fédéral depuis 2004, la BAC est également en charge du management de crise national et prestataire de service pour l'informatique du DDPS. La BAC compte actuellement 660 collaborateurs répartis sur 15 sites dans toute la Suisse.

[17] Art. 11, let. h, Org-DDPS du 7 mars 2003, RS 172.214.1.

[18] La base légale y relative est constituée par l'ordonnance du 15 octobre 2003 sur la guerre électronique (OGE), RS 510.292.

[19] Voir à ce sujet le rapport de la Délégation des commissions de gestion des Chambres fédérales du 10 novembre 2003 relatif au système d'interception des communications par satellite du Département fédéral de la défense, de la protection de la population et des sports (projet «Onyx»), FF 2004, 1377; voir également le rapport de la Délégation des commissions de gestion des Chambres fédérales du 9 novembre 2007 sur la légalité et l'efficacité du système d'exploration radio «Onyx», FF 2008, 2293.

rant, les informations ainsi recueillies sont transmises au commanditaire au sein de la sphère de sécurité de la Confédération pour être analysées. La saisie et la transmission ont lieu conformément aux conventions de prestations conclues à cette fin avec les services intéressés[20]. La FUB procède au tri et au classement de chaque information obtenue sur la base d'un mandat; il identifie ensuite dans le cadre de ses compétences les découvertes fortuites et les transmet aux autres services compétents[21]. Les commanditaires directs sont actuellement le Service de renseignement stratégique (SRS) du DDPS, le Service de renseignement militaire (RM) de l'Etat-major de conduite de l'armée, ainsi que le Service d'analyse et de prévention (SAP) de l'Office fédéral de la police (fedpol)[22]. Les commanditaires directs peuvent, par des conventions de prestations limitées, mettre à disposition d'autres services (par ex. la Centrale nationale d'alarme) les informations recueillies par l'exploration radio permanente. L'analyse et une éventuelle transmission des informations sont de la compétence exclusive des commanditaires et ne peuvent avoir lieu que dans le respect des bases légales sur lesquelles se fonde leur activité.

A la requête de la DélCdG, son président, le Conseiller aux Etats Hans Hofmann, a soumis le 13 mars 2007 l'initiative parlementaire intitulée «Transfert des tâches des services de renseignement civils à un département» (in. parl. 07.404). La DélCdG a été chargée d'élaborer un texte de loi qu'elle a présenté en février 2008[23]. Son entrée en vigueur est prévue pour 2009. Les modifications légales proposées portent pour l'essentiel sur des questions d'organisation et visent à permettre de subordonner les services civils de renseignement au même département. Cela aurait pour conséquence d'une part de soustraire le SRS en tant que service civil à l'emprise de la loi militaire et de créer une base légale spécifique appropriée pour autoriser la récolte à des fins civiles de renseignements à l'étranger. D'autre part, en adaptant la loi fédérale instituant des mesures visant au maintien de la sûreté intérieure, il importe de s'assurer que le SAP soit désigné comme un service du Département de justice et police en vertu de cette loi-ci et non en vertu d'une quelconque loi lorsqu'il agit comme service de renseignement.

A côté de ces services, il existe au sein de l'Etat-major de conduite de l'armée un domaine des opérations en matière d'information. Ce domaine garantit les mesures de défense au niveau des informations d'opérations militaire. Il est responsable de toute la chaîne des opérations (opérations, instruction et développement) et représente ainsi l'organe d'exécution de l'armée dans ce domaine.

2. Bases légales pour recourir à des CNO

2.1. Bases légales pour les CND

La notice «Recht Verteidigung» publiée le 19 février 2008 par le domaine Affaires juridiques du DDPS mentionne comme fondements légaux du CND la loi militaire

[20] Art. 3, al. 3, OGE.

[21] Art. 5, al. 3, OGE.

[22] Faisant usage de son autonomie dans l'organisation de l'administration fédérale (art. 8, al. 1, LOGA ; RS 172.010), le Conseil fédéral a décidé le 21 mai 2008 de transférer le SAP au DDPS dès le 1er janvier 2009. La loi fédérale du 3 octobre 2008 sur le renseignement civil (LFRC) prévoit quant à elle que le SAP et le SRS sont subordonnés au même département; délai référendaire pour cette loi: 22 janvier 2009; FF 2008, 7489. Voir aussi l'initiative parlementaire Transfert des tâches des services de renseignement civils à un département Rapport de la Commission de gestion du Conseil des Etats du 29 février 2008, FF 2008, 3609; avis du Conseil fédéral du 23 avril 2008, FF 2008, 3629. Lors de la mise au point du présent avis de droit, un message complémentaire (LMSI II) était en préparation pour éliminer les divergences matérielles et de technique législative avec le Message du 15 juin 2007 relatif à la modification de la loi fédérale instituant des mesures visant au maintien de la sûreté intérieure; pour plus de détails voir 2.2.5.

[23] Loi fédérale du 3 octobre 2008 sur le renseignement civil (LFRC).

prise «dans son acception la plus large» et l'ordonnance du 26 septembre 2003 sur l'informatique et la télécommunication dans l'administration fédérale (Ordonnance sur l'informatique dans l'administration fédérale, OIAF)[24].

L'OIAF précise à son art. 2, al. 3, que les directives relatives à l'informatique mentionnées dans la présente ordonnance ne s'appliquent pas à l'informatique du domaine de l'armement, ni aux systèmes de conduite et d'engagement de l'armée.

L'art. 9 (sécurité) de l'ordonnance du 15 septembre 1997 concernant l'informatique au Département fédéral de la défense, de la protection de la population et des sports[25] (Ordonnance INF DDPS)[26] ne saurait pas davantage entrer en ligne de compte puisqu'il renvoie à l'OIAF.

Bien que l'ordonnance du 15 octobre 2003 sur la guerre électronique (OGE)[27] fasse aussi référence à la „guerre électronique" à son art. 1, al. 1, ce qui permettrait d'y inclure les CNO, force est de constater que l'OGE a essentiellement pour objet de régler l'„exploration radio permanente". Il en découle que l'OGE ne renferme aucune disposition expresse applicable aux CND et aux CNE ou aux CNA.

En vertu de l'art. 1, al. 2, LAAM, l'armée a pour mission d'assurer la défense de la Suisse et de sa population. L'art. 92 stipule par ailleurs que, pendant l'engagement, la troupe dispose des pouvoirs nécessaires à l'accomplissement de ses missions. L'une d'entre elles est précisée à l'art. 100, al. 1, let. b, LAAM: le service de sécurité militaire (Séc mil) doit veiller à la sécurité informatique. Selon notre conception des CND, nous sommes d'avis que cette dernière disposition constitue une base légale suffisante pour autoriser la Séc mil à recourir aux CND. En vertu de son autonomie d'organisation[28], le Conseil fédéral ou le chef du Département peut confier la charge de la sécurité informatique à une autre unité à l'intérieur de son Département en plus de ses attributions. Cette prérogative ne serait exclue que si l'Assemblée fédérale avait restreint expressément cette compétence organisationnelle du Conseil fédéral, ce qui n'est actuellement pas le cas.

2.2. Conditions de base en droit interne pour recourir à des CNO

2.2.1. Principes de l'activité de l'Etat régi par le droit et compétence fédérale

2.2.1.1. Conditions fixées dans la Constitution fédérale

Chaque fois que l'Etat agit, il doit se conformer à l'art. 5 Cst.[29]. Les principes de la légalité, du respect de l'intérêt public et de la proportionnalité sont applicables à tous les organes étatiques et à tous les domaines de l'activité étatique[30]. Contrairement

[24] RS 172.010.58.

[25] A l'occasion, il conviendrait de compléter le titre dans le Recueil systématique (RS).

[26] RS 510.211.2.

[27] RS 510.292.

[28] Art. 8 LOGA.

[29] La teneur de cette disposition est la suivante:

Art. 5 Principes de l'activité de l'Etat régi par le droit

[1] Le droit est la base et la limite de l'activité de l'Etat.

[2] L'activité de l'Etat doit répondre à un intérêt public et être proportionnée au but visé.

[3] Les organes de l'Etat et les particuliers doivent agir de manière conforme aux règles de la bonne foi.

[4] La Confédération et les cantons respectent le droit international.

[30] Voir par ex. YVO HANGARTNER, in: Commentaire St-Gallois (n. 10), Art. 5 RZ. 5 ss, 30 ss, 35 ss. Et les notes y relatives; GERHARD SCHMID/FELIX UHLMANN, Idee und Ausgestaltung des Rechtsstaates, in: Verfassungsrecht der Schweiz/Droit constitutionnel suisse, édité par Daniel Thürer/Jean-François Aubert/Jörg Paul Müller, Zurich 2001, p. 226 s.

aux cantons, l'activité de l'Etat doit en outre résulter d'une attribution spécifique (expresse ou implicite) de compétences de niveau constitutionnel[31]. Compte tenu de ce qui précède, il faut que l'activité de l'armée repose sur une base légale, qu'elle respecte les principes généraux du droit, qu'elle ne viole pas le droit international public, qu'elle réponde à un intérêt public, qu'elle soit proportionnée au but visé et qu'elle relève d'un domaine de compétence de la Confédération.
La compétence fédérale n'étant pas contestée en l'espèce (défense du pays et sécurité extérieure)[32], elle ne sera pas examinée plus avant dans cet exposé.

2.2.1.2 Domaine d'application territorial des conditions de droit constitutionnel

Dans le contexte actuel, l'art. 5 Cst. revêt une importance toute particulière lorsqu'il touche à l'activité exercée par des organes étatiques suisses. Le fait qu'une partie des CNO – spécialement les CNE et les CNA – se déroule techniquement parlant en dehors du territoire national de la Suisse[33] importe peu eu égard aux obligations imposées par le droit constitutionnel aux organes fédéraux chargés de ces activités[34]. En effet, d'une part ces organes ont leur siège sur le territoire national suisse, y exercent leurs activités et sont donc soumis au droit suisse, d'autre part, ils agissent en tant qu'organes de la Confédération et sont soumis aux principes constitutionnels indépendamment du lieu où s'exerce leur activité ou de celui où elle déploie ses effets.

2.2.1.3. Droits fondamentaux

2.2.1.3.1. En général

La mise en œuvre des CNO (opérations dans les réseaux) touche d'emblée à des domaines protégés par deux droits fondamentaux capitaux garantis par la Constitution. L'art. 13 Cst. protège la sphère privée[35]. La teneur de cette disposition reprend en substance celle de l'art. 8 de la Convention européenne des droits de l'homme (CEDH) qui est également contraignante pour la Suisse[36]. L'art. 16 Cst.[37] protège les libertés d'opinion et d'information. Là encore, une garantie similaire figure dans la CEDH dont l'art. 10 protège la liberté d'expression[38]. Compte tenu de l'évolution de

---

[31] RAINER J. SCHWEIZER, in: Commentaire St-Gallois (n. 10), Art. 3, Rz. 10 s. et les renvois y relatifs.

[32] Cf. art. 54 et 58 Cst.

[33] Voir à ce sujet le rapport essentiel de la DélCdG sur le système Onyx (n. 19), p.1403 ss.

[34] Cf. à ce sujet aussi BVerfGE 100, 313 – Surveillance des télécommunications I: le Tribunal constitutionnel allemand s'est prononcé sur l'application extraterritoriale de garanties fondamentales accordées par la loi: le domaine de protection territorial du secret des télécommunications n'est pas limité au pays (en l'occurrence à l'Allemagne). L'art. 10 GG (Grundgesetz) peut également trouver application lorsqu'une communication qui s'est déroulée à l'étranger a un lien de rattachement suffisamment étroit avec le pays dont l'activité étatique a consisté à procéder à une écoute et à une analyse de cette communication (principe n°2).

[35] La teneur de cette disposition est la suivante:

Art. 13 Protection de la sphère privée

[1] Toute personne a droit au respect de sa vie privée et familiale, de son domicile, de sa correspondance et des relations qu'elle établit par la poste et les télécommunications.

[2] Toute personne a le droit d'être protégée contre l'emploi abusif des données qui la concernent.

[36] CEDH, RS 0.101; voir aussi à ce sujet MARK E. VILLIGER, Handbuch der Europäischen Menschenrechtskonvention, 2ème éd., Zurich 1999, Rz. 554; ARTHUR HAEFLIGER/FRANK SCHÜRMANN, Die europäische Menschenrechtskonvention und die Schweiz, 2ème éd., Berne 1999, p. 248 ss.

[37] La teneur de cette disposition est la suivante:

Art. 16 Libertés d'opinion et d'information.

[1] La liberté d'opinion et la liberté d'information sont garanties.

[2] Toute personne a le droit de former, d'exprimer et de répandre librement son opinion.

[3] Toute personne a le droit de recevoir librement des informations, de se les procurer aux sources généralement accessibles et de les diffuser.

[38] S. VILLIGER (n. 35), Rz. 603 ss.

la technique, il n'est pas à exclure que d'autres droits fondamentaux puissent être touchés.

Au titre de la protection de la sphère privée, l'art. 13, al. 1, Cst. protège expressément les particuliers contre des contrôles et des consultations non autorisés de la correspondance et des relations qu'ils établissent par la poste et par les télécommunications. Cette réglementation trouve son équivalent à l'art. 8, ch. 1, CEDH. Diverses décisions rendues dans ce domaine par la Cour Européenne des Droits de l'Homme[39] ainsi que par le Tribunal fédéral[40] sont déterminantes pour apprécier la portée et le mode d'application de ce droit fondamental.

La doctrine et la jurisprudence ont depuis toujours considéré que la protection des relations établies par télécommunication relevait de la protection de la sphère privée et non pas de la liberté d'opinion et d'information[41]. C'est pourquoi nous ne traiterons pas plus avant des points qui pourraient toucher à la liberté d'opinion ou à la liberté d'information garanties par l'art. 16 Cst.

La protection assurée par le biais de la garantie des droits fondamentaux n'est pas absolue, sous réserve de leur essence qui est intangible[42]. L'art. 36 Cst.[43] subordonne les restrictions d'un droit fondamental par les autorités à l'existence d'une base légale, à celle d'un intérêt public suffisant et au respect du principe de la proportionnalité. Il s'agit-là des conditions nécessaires à la restriction des libertés individuelles[44]. Par base légale, on entend généralement, dans ce contexte, une réglementation abstraite, c'est-à-dire une norme juridique[45]. L'art. 164, al. 1, let. b, précise en outre que toutes les dispositions importantes qui fixent des règles de droit – soit en particulier les dispositions fondamentales relatives à la restriction des droits constitutionnels – doivent être édictées sous la forme d'une loi sujette au référendum. Sur ce

[39] Cf. l'arrêt de la Cour Européenne des Droits de l'Homme (CEDH) du 24 avril 1990 dans l'affaire *Kruslin* contre France. Dans cet arrêt, il est précisé que les écoutes et autres formes d'interception des entretiens téléphoniques représentent une atteinte grave au respect de la vie privée et de la correspondance, que, partant, elles doivent se fonder sur une loi d'une précision particulière et que l'existence de règles claires et détaillées en la matière apparaît indispensable, d'autant que les procédés techniques utilisables ne cessent de se perfectionner (§ 33). Cf. aussi les arrêts *Malone* contre Royaume-Uni du 2 août 1984 (§ 67), *Huvig* contre France du 24 avril 1990 (§ 29) et *Amman* contre Suisse du 16 février 2000 (§ 58). A l'heure actuelle, la jurisprudence de la CEDH a surtout trait à des écoutes téléphoniques ordonnées par une autorité judiciaire ou administrative sous la juridiction de laquelle se trouvent les citoyens visés par cette mesure. La CEDH a précisé à plusieurs reprises que la responsabilité des Etats contractants n'était pas seulement limité à leur territoire national, mais aussi „ […] que la notion de «juridiction» au sens de l'article 1 de la Convention ne se circonscrit pas nécessairement au seul territoire national des Hautes Parties contractantes […]. La Cour a admis que, dans des circonstances exceptionnelles, les actes des Etats contractants accomplis ou produisant des effets en dehors de leur territoire peuvent s'analyser en l'exercice par eux de leur juridiction au sens de l'article 1 de la Convention." (Arrêt du 8 juillet 2004 dans l'affaire *Ilascu et autres* contre Moldova et Russie (§ 314)); et encore l'arrêt du 23 mars 1995 dans l'affaire *Loizidou* contre Turquie (§ 62). Le critère factuel déterminant est constitué par le "contrôle effectif" exercé sur la personne visée (à ce sujet: JUAN ANTONIO CARRILLO-SALCEDO, in Pettiti, Decaux, Imbert, La Convention européenne des droits de l'homme, Paris 1995, p. 136). Même si la CEDH n'a pas encore eu l'occasion de se prononcer sur le thème des écoutes effectuées par un Etat partie à la Convention européenne des droits de l'homme sur le territoire d'un autre Etat, il y a lieu d'admettre que les garanties accordées par la Convention s'appliquent.

[40] ATF 115 Ia 299; HAEFLIGER/SCHÜRMANN (n. 35), p. 44.

[41] Voir aussi JÖRG PAUL MÜLLER, Grundrechte in der Schweiz, 3ème éd., Berne 1999, p.42 ss et 131 ss.

[42] Voir à ce sujet RAINER J. SCHWEIZER, in: Commentaire St-Gallois (n. 10), Art. 36, Rz. 28 s. et renvois.

[43] La teneur de cette disposition est la suivante:

Art. 36 Restriction des droits fondamentaux.

[1] Toute restriction d'un droit fondamental doit être fondée sur une base légale. Les restrictions graves doivent être prévues par une loi. Les cas de danger sérieux, direct et imminent sont réservés.

[2] Toute restriction d'un droit fondamental doit être justifiée par un intérêt public ou par la protection d'un droit fondamental d'autrui.

[3] Toute restriction d'un droit fondamental doit être proportionnée au but visé.

[4] L'essence des droits fondamentaux est inviolable.

[44] ULRICH HÄFELIN/WALTER HALLER/HELEN KELLER, Schweizerisches Bundesstaatsrecht, 7ème éd., Zurich 2008, Rz. 302 s.; RAINER J. SCHWEIZER, in: Commentaire St-Gallois (n. 10), Art. 36, Rz. 7 et les renvois y relatifs.

[45] HÄFELIN/HALLER/KELLER (n. 43), Rz. 308 ss; SCHWEIZER (n. 43), Rz. 10 s.

point, les conditions de la Constitution sont plus sévères que celles de la CEDH, cette dernière considérant une simple norme matérielle comme admissible[46], sauf en cas de restrictions importantes où la norme doit alors être dans une certaine mesure concrète, c'est-à-dire précise et prévisible[47].

2.2.1.3.2. Protection de la sphère privée

L'engagement pris par les autorités de garantir le secret postal et le secret des télécommunications constitue une manifestation spécifique de la protection du droit fondamental de la personnalité en vertu de laquelle toute intrusion injustifiée dans la sphère privée d'une personne doit être proscrite[48]. La protection ne dépend dès lors ni du contenu de l'information ni de son support, en sorte qu'elle est accordée tant à une correspondance privée ou professionnelle qu'à une communication par courriel ou par sms[49].
Une base légale est nécessaire pour autoriser les autorités à accéder à des informations dont la transmission est protégée par l'art. 13, al. 1, Cst. L'examen de la légalité d'un accès à des informations de tiers transmises par voie électronique soulève la question de savoir si cet accès constitue une restriction grave au sens de l'art. 36, al. 1, Cst. et s'il doit être défini dans une loi formelle, ne serait-ce que dans son principe. A défaut d'en avoir informé les personnes intéressées et de leur avoir accordé une voie formelle de recours, toute forme d'intrusion par les autorités dans une communication privée ou dans des données personnelles qui n'ont jamais été conçues pour être divulguées de quelque manière que ce soit constitue une atteinte grave à la sphère privée protégée par le droit et requiert l'existence d'une base légale formelle[50].

2.2.2. Bases légales pour les CNE

Ainsi que nous l'avons déjà exposé[51], il existe une base légale suffisante pour recourir aux CND.

De la même manière[52], il a été démontré qu'il est nécessaire de créer une base légale pour recourir aux CNA en temps de paix, ce qui nous amène à conclure que les CNA ne peuvent trouver application qu'en temps de guerre et, en principe, par les soins de l'armée.

En revanche, il n'y a aucune base légale pour justifier les CNE en dehors du service actif. Eu égard aux conditions décrites au ch. 2.2.1.3, l'art. 99 LAAM ne constitue pas une base légale formelle suffisante pour recourir à des CNO[53]. Tout d'abord parce

[46] SCHWEIZER (n. 44), Rz. 13-15 et les renvois y relatifs; cf. aussi JOCHEN ABR. FROWEIN/WOLFGANG PEUKERT, EMRK-Kommentar, 2ème éd., Kehl/Strasbourg/Arlington, 1996, Art. 5 Rz. 26.

[47] Jens MEYER-LADEWIG, EMRK-Handkommentar, 2ème éd., Baden-Baden 2006, N° 10 ad art. 8.

[48] MÜLLER (Fn. 40), p. 132; VILLIGER (Fn. 36), Rz. 564.

[49] STEPHAN BREITENMOSER, in: Commentaire St-Gallois (n. 10), Art. 13, Rz. 34 s.; CHRISTOPH GRABENWARTER, Europäische Menschenrechtskonvention, 3ème éd., Munich/Bâle/Vienne 2007, § 22, Rz 24.

[50] BREITENMOSER (n. 48), Art. 13, Rz. 35; GIOVANNI BIAGGINI, BV-Kommentar, Zurich 2007, Art. 13, Rz. 10; cf. ATF 126 I 50 sur la surveillance du courrier électronique.

[51] Voir ch. 2.1.

[52] Voir ch. 1.3.

[53] La teneur de cette disposition est la suivante:

Art. 99 Service de renseignements.

[1] Le service de renseignements a pour tâche de rechercher, d'évaluer et de diffuser des informations sur l'étranger importantes en matière de politique de sécurité.

[2] Il est habilité à traiter, le cas échéant à l'insu des personnes concernées, des données personnelles, y compris des données sensibles et des profils de la personnalité, à condition et aussi longtemps que ses tâches l'exigent. Il peut, de cas en cas, communiquer des données personnelles à l'étranger en dérogation aux dispositions de la protection des données.

que l'al. 1 ne décrit que les tâches dévolues au service de renseignements, ensuite parce que l'al. 2 pose les conditions légales à respecter pour la récolte d'informations. Quant à la délégation de compétences énoncée à l'al. 3, elle ne satisfait pas aux exigences d'une base légale formelle pour justifier le recours à des CNO. En effet, ainsi que nous l'avons évoqué, les CNE doivent être fondées sur une base légale formelle. C'est du reste pour cette même raison qu'une base légale est en voie de création pour autoriser l'exploration radio (système Onyx)[54].

Si l'on souhaitait donner aux organes de renseignements de l'armée la possibilité de recourir aux CNE, il faudrait créer une base légale appropriée. Lors de l'élaboration de cette base légale, il conviendrait, en particulier, de s'inspirer du procédé similaire observé par le SAP[55] en matière de perquisition secrète d'un système informatique.

2.2.3. Intérêt public

La récolte d'informations opérée par l'armée (CNE) doit être fondée en principe sur l'intérêt public[56]. De l'avis de la doctrine et de la jurisprudence, le maintien des sécurités intérieure et extérieure ainsi que les questions de sécurité qui ont trait à la défense nationale sont par définition d'un intérêt public important[57]. Il en va de même de la sphère privée protégée par l'art. 13 Cst. et par l'art. 8 CEDH. Il importe dès lors de procéder à une pesée minutieuse des intérêts en faveur de la sécurité et de ceux, publics et privés qui s'y opposent, en faveur de l'inviolabilité de la sphère privée[58].

2.2.4. Proportionnalité

Pour savoir dans quelle mesure la collecte d'informations effectuée par l'armée au moyen du CNE au profit des organes du renseignement militaire sont conformes au précepte constitutionnel de la proportionnalité, il faut, selon l'avis de la doctrine et de la jurisprudence, les examiner à la lumière des trois conditions incluses dans ce précepte: adéquation de la mesure par rapport au but visé, nécessité de la mesure et proportionnalité entre le but poursuivi par la mesure et ses effets[59]. Par la même occasion, il convient de signaler que dans le cadre de l'examen de la proportionnalité que le Tribunal fédéral effectue librement, celui-ci a fait montre d'une grande retenue

---

[2bis] Il peut communiquer au Service d'analyse et de prévention et à l'Office fédéral de la police des informations sur des personnes en Suisse qu'il a obtenues dans l'exercice des activités mentionnées à l'al. 1, et qui peuvent être importantes pour la sûreté intérieure ou la poursuite pénale.

[3] Le Conseil fédéral règle:

a. le détail des tâches du service de renseignements, son organisation et la protection des données;

b. l'activité du service de renseignements en période de service de promotion de paix, de service d'appui et de service actif;

c. la collaboration du service de renseignements avec les autres services cantonaux et fédéraux ainsi qu'avec les services étrangers;

d. les exceptions aux dispositions sur l'enregistrement des fichiers lorsque, à défaut, la recherche des informations serait compromise.

[4] La protection des sources doit dans tous les cas être assurée.

[5] Le service de renseignements est directement subordonné au chef du Département de la défense, de la protection de la population et des sports.

[54] Voir ch. 2.2.5.

[55] Voir ch. 2.2.5: limites à l'art. 18, let. m, LMSI II.

[56] Sur cette notion voir notamment MARTIN PHILIPP WYSS, Öffentliches Interesse – Interessen der Öffentlichkeit? Das öffentliche Interesse im schweizerischen Staats- und Verwaltungsrecht, Berne 2001, Rz. 1 ss; ULRICH HÄFELIN/GEORG MÜLLER/FELIX UHLMANN, Allgemeines Verwaltungsrecht, 5ème éd., Zurich/St-Gall 2006, Rz. 535 ss.

[57] WYSS, (n. 55), Rz. 199 ss.; HÄFELIN/MÜLLER/UHLMANN (n. 55), Rz. 544 ss. et les renvois y relatifs.

[58] Voir notamment HÄFELIN/MÜLLER/UHLMANN (n. 55), Rz. 562 ss; WYSS (n. 55), Rz. 517 ss.

[59] Voir à ce sujet HÄFELIN/MÜLLER/UHLMANN (n. 55) Rz. 581 ss.

quant à l'appréciation des faits et quant à la pesée des intérêts publics en présence[60].

Si l'on examine la question de l'adéquation de la récolte d'informations requise par la FUB au moyen du CNE, on peut conclure, au vu des indications fournies par les services concernés, que le système permet de filtrer des informations isolées ayant trait à la sécurité sur des réseaux informatiques ou des ordinateurs individualisés lorsqu'il existe des motifs de suspicion et que les conditions nécessaires sont réunies. Il va de soi que les services compétents ont à se prononcer sur la valeur intrinsèque de ces informations et doivent les apprécier à la lumière des circonstances du cas d'espèce, mais cela ne remet pas en cause la question de principe de l'adéquation des mesures.

Le principe de la nécessité de la mesure implique celui de l'atteinte la moins dommageable au droit fondamental et celui de la prohibition de l'excès par rapport à l'objectif visé[61]. Si l'on tient compte de la rapidité de l'évolution sur le plan international, il ne fait aucun doute que la recherche de données informatisées spécifiques sur la situation à l'étranger effectuée par la Confédération pour satisfaire ses besoins dans le domaine de la sécurité répond à une véritable nécessité. Le caractère adéquat de la demande d'enquête et la prohibition de l'excès de la mesure requise doivent être surtout respectés dans le cadre de l'attribution du mandat et au stade de l'élaboration d'une future réglementation sur la sélection, le traitement et l'utilisation des informations recueillies. Cette dernière opération mérite d'être mentionnée tout spécialement en raison du fait que l'on autorise fréquemment l'accès à des données strictement confidentielles stockées par exemple sur un disque dur alors qu'elles n'ont jamais été recueillies pour être divulguées de quelque manière que ce soit.

Sur un plan abstrait, l'examen de la proportionnalité entre le but poursuivi par la mesure et ses effets ne peut être que très limité; il doit plutôt porter sur les modalités de chaque mandat de récolte d'informations et sur l'utilisation de ces informations. Pour apprécier si chaque cas d'espèce respecte le principe de la proportionnalité, il faut notamment examiner la nature des dangers existants, ceux que la récolte d'informations devrait permettre de détourner, ainsi que les conséquences pour les parties visées qui sont entrées en contact par voie de télécommunication. A l'instar de ce qu'il advient lors de la pesée des intérêts publics, le fait que les personnes effectivement touchées par les CNE n'en sont généralement pas informées – ou ne devraient pas l'être – et qu'elles ne sont dès lors pas en mesure de faire part de leurs observations à aucun stade de la procédure influe négativement sur l'examen général de proportionnalité. Ce défaut, qui est en même temps inhérent au but poursuivi par ces opérations, doit être compensé par une procédure de contrôle et d'examen menée au sein des institutions.

La question de savoir si l'intérêt des particuliers à bénéficier en premier lieu d'une protection illimitée des moyens de communication électroniques privés doit primer l'intérêt public de l'Etat à pouvoir accéder aux informations stockées dans des réseaux préalablement définis ne peut être clairement tranchée sur un plan général. Pour ce faire, il convient de procéder à un examen au cas par cas lors de l'attribution des mandats à la FUB et du traitement des données qui auront pu être récoltées[62].

La procédure usuelle décrite par l'OCGE devrait *de lege ferenda* suffire à dissiper les craintes suscitées par le fait que les autorités qui requièrent l'enquête sont en pratique aussi celles qui procèdent à la pesée des intérêts en présence en vue de

[60] Cette décision était fondée en l'espèce sur des implications de politique de sécurité intérieure et extérieure; ATF 129 II 192, 208; confirmé dans ATF 132 I 229, 244.

[61] HÄFELIN/MÜLLER/UHLMANN (n. 55), Rz. 591 s.

[62] Cf. notamment HÄFELIN/MÜLLER/UHLMANN (Fn. 55), Rz. 564.

l'utilisation du matériau informatif récolté et ce, sans qu'il soit accordé à la personne touchée la possibilité de s'exprimer et sans que des voies de recours et des contrôles indépendants soient officiellement aménagés. Il est, par ailleurs, compréhensible que des CNE soient entreprises sans que les personnes touchées en soient informées et sans qu'elles puissent prêter leur concours. D'autre part, les mesures compensatoires proposées pour assurer une mise en balance impartiale des intérêts par le biais d'un contrôle indépendant de la récolte et de l'exploitation des informations ne sont pas davantage admissibles[63]. Compte tenu de la proximité des services de renseignement avec les autorités exécutives, la CEDH, en se fondant sur l'art. 13 de la Convention européenne des droits de l'homme, exige qu'un contrôle judiciaire soit assuré à tout le moins en dernier ressort dans les cas ordinaires[64].

2.2.5. Limites posées par l'art. 18, let. m, LMSI II

L'actuel art. 14, al. 2, LMSI, définit de manière exhaustive les moyens qui peuvent être mis en œuvre aux fins de la recherche d'informations pour le compte du SAP; les opérations relatives aux CNO n'y figurent pas[65]. Celles-ci ne devraient être autorisées que sur la base de la LMSI II, à l'état de projet. La perquisition secrète d'un système informatique en vertu de l'art. 18, let. m, LMSI II – soit les opérations assimilées à des CNE – sera réglementée en ce sens que le SAP pourra perquisitionner des systèmes informatiques utilisés par des perturbateurs présumés et dont ils peuvent disposer[66].

L'adoption de la LFRC a conduit le Parlement à modifier la LAAM[67] en donnant une nouvelle teneur à l'art. 99[68]. Mentionnons cependant que cette dernière ne prend pas

---

[63] CEDH, arrêt du 6 juin 2006 dans l'affaire *Segerstedt-Wiberg et autres* contre Suède (§ 103 [jurisprudence constante]).

[64] CEDH, arrêt du 4 mai 2000 dans l'affaire *Rotaru* contre Roumanie (§ 59): „ […] pour que les systèmes de surveillance secrète soient compatibles avec l'article 8 de la Convention, ils doivent contenir des garanties établies par la loi et qui sont applicables au contrôle des activités des services concernés. Les procédures de contrôle doivent respecter aussi fidèlement que possible les valeurs d'une société démocratique, en particulier la prééminence du droit, à laquelle se réfère expressément le préambule de la Convention. Elle implique, entre autres, qu'une ingérence de l'exécutif dans les droits de l'individu soit soumise à un contrôle efficace que doit normalement assurer, au moins en dernier ressort, le pouvoir judiciaire, car il offre les meilleures garanties d'indépendance, d'impartialité et de procédure régulière (arrêt Klass et autres précité, pp. 25-26, § 55)" ; de même *Segerstedt-Wiberg et autres* contre Suède (n. 62), § 121 s.

[65] La teneur de cette disposition est la suivante:

Des données personnelles peuvent être recueillies par le biais:

a. de l'exploitation de sources accessibles au public;
b. de demandes de renseignements;
c. de la consultation de documents officiels;
d. de la réception et de l'exploitation de communications;
e. d'enquêtes sur l'identité ou le lieu de séjour de personnes;
f. de l'observation de faits, y compris au moyen d'enregistrements d'images et de sons, dans des lieux publics et librement accessibles;
g. du relevé des déplacements et des contacts de personnes.

[66] Teneur de la disposition:

Art. 18m (nouveau) Perquisition secrète d'un système informatique

Si des faits ou des incidents précis et récents laissent supposer qu'un perturbateur présumé utilise un système informatique dont il peut disposer et qui est spécialement protégé contre tout accès indu, l'office fédéral peut procéder à une perquisition du système informatique. La perquisition peut avoir lieu à l'insu du perturbateur présumé.

[67] Voir n. 22.

[68] La teneur de cette disposition est la suivante:

Art. 99, al. 1, 2bis, 3, let. c, 4 et 5

[1] Le service de renseignements militaire (service de renseignements) a pour tâche de rechercher et d'évaluer des informations sur l'étranger importantes pour l'armée, notamment du point de vue de la défense nationale, du service de promotion de la paix et du service d'appui à l'étranger.

[2bis] Il peut communiquer aux autorités de poursuite pénale de la Confédération les informations sur des personnes en Suisse qu'il a obtenues dans l'exercice des activités mentionnées à l'al. 1, et qui peuvent être importantes pour la poursuite pénale. Le Conseil fédéral règle les modalités.

[3] Le Conseil fédéral règle:

[…]

encore en considération les propositions de modification résultant du message complémentaire sur la LMSI II qui ont principalement trait à l'introduction d'une base légale pour l'exploration radio. Cette version de l'art. 99 LAAM ne satisfait pas non plus aux exigences légales formelles pour les CNO[69].

Le droit de procéder à une perquisition secrète d'un système informatique n'appartiendrait qu'au SAP et en aucun cas au SRS et au RM, même après la réunion de ces derniers sous le toit du DDPS. En effet, en dépit du fait que le SRS sera réuni au SAP au sein du DDPS, il convient de souligner que les tâches de ces deux services telles qu'elles sont définies par la loi ne sont toujours pas similaires. En vertu de l'art. 5, al. 2, de l'ordonnance sur l'organisation des services de renseignements au sein du Département fédéral de la défense, de la protection de la population et des sports (Ordonnance sur les services de renseignements au DDPS, Orens) du 26 septembre 2003[70], les services de renseignements du DDPS conviennent d'un règlement de collaboration qui doit être approuvé par le chef du DDPS.

En d'autres termes, la décision du Conseil fédéral de subordonner les services de renseignements du SAP au chef du DDPS (arrêté du Conseil fédéral du 21.05.2008) ne change rien aux tâches distinctes qui sont dévolues par la loi à ces deux services. Une collaboration plus étroite n'est admissible que dans les limites des dispositions légales en vigueur.

Les CNO effectuées dans le cadre de l'armée à la demande des autorités civiles doivent respecter la réserve de l'art. 1, al. 3, LAAM, qui n'autorise ces opérations que lorsque les forces de police ne suffisent plus pour faire face aux menaces graves contre la sécurité intérieure (let. a) ou pour maîtriser d'autres situations extraordinaires, en particulier en cas de catastrophe dans le pays ou à l'étranger (let. b). Par la même occasion, il convient de relever que toute attaque d'un réseau informatique – même important – ne constitue pas nécessairement une attaque militaire[71].

3. Limites imposées aux CNO par le droit international public

3.1. Introduction et présentation générale

Les questions concrètes posées par la Délégation des Commissions de gestion ne se rapportent pas directement au droit international public (DIP). Toutefois, dans son courrier du 20 mai 2008, le DDPS a prié la Direction du droit international public de clarifier également les questions qui se posent en droit international public.

En conséquence, la deuxième partie du présent avis de droit relève les questions de droit international public posées par les *Computer Network Operations*. Quand bien même il est impossible d'y apporter des réponses définitives, les pages qui suivent

---

c. la collaboration du service de renseignements avec les autres services cantonaux et fédéraux ainsi qu'avec les services étrangers; il approuve les accords administratifs internationaux conclus par le service de renseignements et veille à ce que ces accords ne soient exécutoires qu'après l'obtention de l'approbation;

[4] Le Conseil fédéral règle la protection des sources en fonction de leurs besoins de protection effectifs. Les personnes qui sont en danger en raison de leurs activités de renseignement sur l'étranger doivent être protégées dans tous les cas.

[5] Le Conseil fédéral règle la subordination du service de renseignements. Il veille à ce que la légalité, l'opportunité et l'efficacité de l'activité du service de renseignements soient contrôlées. Le département compétent établit un plan de contrôle annuel qu'il coordonne avec les contrôles parlementaires.

[69] Voir ch. 2.2.2.

[70] RS 510.291.

[71] Voir ch. 3.2.2.1.

proposent un état des lieux et des éléments de discussion. En tout état de cause, chaque cas doit être étudié individuellement.

L'état des lieux de la question doit être fait pour chaque branche du DIP. Dans un premier temps, il convient de distinguer le *jus ad bellum* et le *jus in bello*.

Le *jus ad bellum*, également appelé *jus contra bellum*, interdit par principe tout emploi de la force armée dans les rapports internationaux. Le recours à la force armée est légitime uniquement dans les cas de légitime défense ou dans le cadre du système de sécurité collective des Nations Unies. Il convient donc de se demander s'il est possible de conduire des opérations dans les réseaux informatiques qui soient légitimes au regard du DIP et dans quels cas. Ce faisant, il est important de considérer que le recours à la force armée à des fins défensives est légitime uniquement lorsqu'il s'agit de réagir à une agression qui atteint le niveau d'intensité d'une agression armée selon l'art. 51 de la Charte des Nations Unies [72]. Si une opération au travers de réseaux informatiques n'atteint pas cette intensité, elle peut néanmoins violer le principe de non-intervention. Celui-ci est en effet plus large que le principe du non-recours à la force : il interdit par principe aux Etats de porter atteinte à la souveraineté d'un autre Etat.

Le *jus in bello*, quant à lui, régit l'utilisation de la force armée dans les conflits armés, sans toutefois répondre à la question de savoir si le fait même de participer à ce conflit armé est légitime au regard du droit international public. Le *jus in bello* correspond au dispositif normatif du droit international humanitaire (DIH). Il faut donc s'interroger sur la manière dont ce dispositif s'applique aux *Computer Network Operations*.

En outre, pour la Suisse, le droit de la neutralité revêt un intérêt particulier. Il soulève la question de savoir quels sont les droits et les devoirs pour un Etat neutre en cas de guerre comportant des opérations au travers de réseaux informatiques.

Il résulte de cet état des lieux que la zone grise entre *Computer Network Defense* (CND) et *Computer Network Attack (*CNA) ne peut pas être examinée pour sa partie relevant du droit international public de la même manière que pour ses aspects relevant des bases légales nationales[73]. Ainsi, selon les règles du *jus ad bellum*, on ne peut pas assimiler les contre-attaques, qui sont défensives, à des CNA, qui sont offensives.

Le tableau reproduit en annexe (graphique 3) récapitule l'état des lieux de la question au regard du droit international public, non sans anticiper sur certains résultats de l'analyse. Il donne d'abord une vue générale des questions de droit international public que posent les CNO ; deuxièmement, il indique où sont traitées les différentes problématiques dans la partie consacrée au droit international ; troisièmement, il intègre les hypothèses préexistantes et certains résultats de l'avis de droit afin de contribuer à une meilleure compréhension du sujet.

3.2. CNO et *jus ad bellum* ou *jus contra bellum*

Aujourd'hui, le recours à la force est absolument proscrit dans les rapports internationaux. Cette interdiction qui repose sur l'art. 2, al. 4, de la Charte des Nations Unies et sur le droit coutumier, fait partie des normes impératives du droit international (*jus cogens*). Les seules exceptions au principe du non-recours à la force admises par la Charte des Nations Unies sont les mesures de sécurité collective (Chapitre VII de la

[72] RS 0.120.

[73] Voir le graphique 1 (CNO) en annexe et les explications au chiffre 1.1. Avant la partie 3, les zones grises ont été surclassées. Ainsi, les contre-attaques en réaction à une CNA de l'adversaire, en particulier, ont été classées dans les CNA dans la partie de l'avis portant sur les bases légales nationales.

Charte) ainsi que la légitime défense individuelle et collective en cas d'agression armée (art. 51 de la Charte)[74].

3.2.1. Interdiction du recours à la force

La première question qui se pose est celle-ci : l'attaque d'un réseau informatique rentre-t-elle dans le champ de l'interdiction du recours à la force ? D'après la doctrine et la jurisprudence dominantes, le principe du non-recours à la force se rapporte uniquement à l'emploi de la force armée entre Etats. Pour répondre à la question, il faut donc d'abord établir si l'attaque d'un réseau informatique constitue un recours à la force armée. Dans l'affirmative, il faut alors se demander si l'attaque d'un réseau informatique peut être considérée comme un emploi de la force *entre Etats*.

3.2.1.1 Les attaques de réseaux informatiques constituent-elles un recours à la force armée ?

Un ordinateur peut-il être considéré comme une arme, et une attaque au travers un réseau informatique d'un autre Etat peut-elle être considérée comme un recours à la force armée ?

La discussion à ce sujet dans la doctrine de droit international public n'en est qu'à ses débuts[75]. Cependant, il apparaît déjà que, pour la doctrine, un ordinateur peut devenir une arme et il est imaginable qu'une attaque contre des réseaux informatiques puisse prendre les proportions d'un recours à la force armée.

Dans la notion d'arme, ce n'est pas le moyen employé qui est déterminant, mais l'intention dans laquelle il est utilisé et les effets spécifiques qu'il déploie. Si l'on utilise un ordinateur pour attaquer des réseaux informatiques dans le but de détruire des biens ou de porter atteinte à l'intégrité physique ou à la vie et que les conséquences sont les mêmes que celles de l'emploi physique de la force armée, cette attaque peut être assimilée à un recours à la force armée. Il convient donc d'apprécier les situations au cas par cas. La doctrine cite des exemples comme l'attaque d'une centrale nucléaire qui libèrerait de la radioactivité, la coupure de l'électricité alimentant des hôpitaux non équipés de groupes électrogènes ou encore la manipulation de dispositifs de sécurité dans les transports entraînant des crashs aériens ou des collisions ferroviaires. Ces scénarios d'agression non seulement sont contraires aux principes du droit international humanitaire[76], mais ils rentrent aussi dans le champ de l'interdiction du recours à la force.

On peut aussi penser à d'autres attaques de réseaux informatiques que celles conduisant à un emploi de la force physique. Des attaques informatiques peuvent être conduites dans le but d'exercer une contrainte économique ou politique sur un autre Etat. La doctrine cite comme exemple une attaque contre le système de paiement, le système bancaire ou le système boursier d'un pays.

---

[74] Concernant l'interdiction de l'emploi de la force et les exceptions à cette interdiction, lire ANNE PETERS : *Völkerrecht*, Zurich 2008 ; MICHAEL BOTHE : Friedenssicherung und Kriegsrecht, in : WOLFGANG GRAF VITZHUM (éd.), *Völkerrecht*, Berlin 2007 ; KNUT IPSEN : *Völkerrecht*, Munich 2004 ; WALTER KÄLIN et. al., *Völkerrecht*, Berne 2006.

[75] FALKO DITTMAR : Angriffe auf Computernetzwerke : *‚Jus ad bellum' und ‚jus in bello'*, Berlin 2005 ; MICHAEL N. SCHMITT : „Angriffe im Computernetz und das *jus ad bellum*" in : *Neue Zeitschrift für Wehrrecht*, p. 177 – 195 ; THOMAS C. WINGFIELD : „CNA and the Jus ad Bellum : An Introduction" in : *International Expert Conference on Computer Network Attacks and the Applicability of International Humanitarian Law*, Stockholm 2004 ; D.B. SILVER : Computer Network Attack as a Use of Force Under Article 2 (4) of the United Nations Charter, in : M.N. SCHMITT (éd.), *Computer Network Attack and International Law,* 2002. Il s'agit là d'une question d'interprétation de la Charte des Nations Unies, qui est régie par l'art. 31 de la Convention sur le droit des traités (RS 0.111). En l'espèce, ce sont l'esprit et le but de la Charte des Nations Unies qui sont déterminants.

[76] Voir chiffre 3.4.

La contrainte politique ou économique n'entre pas dans le champ de l'interdiction de l'emploi de la force. Les attaques menées à cette fin ne violent donc pas le principe du non-recours à la force.

En revanche, les attaques contre les réseaux informatiques d'autres Etats n'atteignant pas le niveau d'intensité qui les soumettrait à l'interdiction du recours à la force peuvent violer le principe de la non-intervention, qui est plus étendu que le principe du non-recours à la force[77].

3.2.1.2. Les attaques de réseaux informatiques constituent-elles un emploi de la force entre Etats ?

En principe, l'interdiction du recours à la force s'applique uniquement aux relations entre Etats. Peut-on qualifier une attaque au travers un réseau informatique d'emploi l'emploi de la force entre Etats ? Il est possible que la réponse soit moins aisée à apporter que pour une agression armée classique. En effet, il est parfois très difficile de remonter jusqu'à la source d'une attaque, d'autant qu'un agresseur a la possibilité de prendre des dispositions pour brouiller sa piste.

Mais l'interdiction du recours à la force ne s'applique pas seulement aux confrontations directes entre Etats ; elle vise aussi les confrontations indirectes. Dans son arrêt Nicaragua, la Cour internationale de Justice (CIJ) avait estimé que le soutien apporté à des bandes armées et à des groupes de rebelles armés par la livraison d'armes, la fourniture d'une formation militaire et l'octroi d'une assistance logistique pouvait être considéré comme violant le principe du non-recours à la force (voir également l'arrêt concernant l'Ouganda et le Congo)[78].

On peut concevoir que des attaques de réseaux informatiques constituent un exercice indirect de la force, par exemple si ces opérations consistent à former des pirates informatiques et à leur fournir une assistance et que ces pirates sont à l'origine d'une attaque au travers un réseau informatique qui atteint l'intensité d'un recours à la force armée. Il faut cependant préciser que, selon l'arrêt Nicaragua de la CIJ, l'Etat concerné doit être impliqué de manière importante dans l'acte constitutif de recours à la force non étatique pour que celui-ci puisse être qualifié d'étatique[79].

Lorsqu'un Etat s'abstient d'agir contre un acte d'emploi de la force perpétré à partir de son territoire ou tolère cet acte, dans quelle mesure ce dernier peut-il être qualifié d'emploi de la force ayant un caractère étatique indirect ? La question est controversée[80]. Elle se pose en particulier lorsqu'un Etat n'intervient pas pour empêcher la préparation ou l'exécution d'actes terroristes contre un autre Etat. En principe, un tel comportement ne peut cependant pas être assimilé automatiquement à un recours à la force de l'Etat qui n'intervient pas[81].

L'art. 2, al. 4, de la Charte de l'ONU interdit non seulement le recours à la force, mais aussi la menace de recourir à la force. Ainsi, la CIJ estime dans sa jurisprudence qu'il y a violation de l'art. 2, al. 4 lorsqu'un Etat menace d'employer illicitement la force (avis sur les armes nucléaires)[82]. Il en découle que si une attaque contre un ré-

[77] Voir chiffre 3.3.

[78] CIJ, "Activités militaires et paramilitaires au Nicaragua et contre celui-ci (Nicaragua v. Etats-Unis d'Amérique)", *C.I.J Recueil* 1986 ; CIJ, "Activités armées sur le territoire du Congo (Réublique démocratique du Congo c. Ouganda)", *C.I.J. Recueil* 2005 ; voir aussi PETERS (N. 67), p. 285 ss. ; IPSEN (N. 67), p. 1076 et 1087 ; BOTHE (N. 67), p. 648 s.

[79] Voir aussi *Projets d'articles sur la responsabilité des Etats pour les faits internationalement illicites*, adoptés par la C.D.I., Comité de rédaction en deuxième lecture, 53ème sess., U.N. Doc.A/CN.4/L.602/Rev.1 (2001).

[80] Cf. ibid.

[81] Pour plus de détails, voir chiffre 3.2.2.4.

[82] ICJ, "Licéité de la menace ou de l'emploi d'armes nucléaires", Avis consultatif, *C.I.J. Recueil* 1996. Pour une discussion plus poussée, lire STÜRCHLER Nikolas : *The Threat of Force in International Law*, Cambridge 2007.

seau informatique peut être qualifiée de violation du principe de non-recours à la force, la menace d'exécuter cet acte de force est, elle aussi, illicite.

La pratique de la dissuasion par une préparation à la défense n'est pas considérée comme contraire au droit international public car la menace de recours à la force qui lui est sous-jacente est limitée à la légitime défense, qui est licite. Ce raisonnement pose problème dans la mesure où il n'est pas toujours possible d'établir une distinction entre l'armement à des fins de défense et l'armement à des fins d'agression.

Conclusion : *Les attaques de réseaux informatiques violent le principe du non-recours à la force s'ils ont des effets identiques à l'exercice physique de la force armée. Cela s'applique au recours à la force ayant un caractère étatique, qu'il soit direct ou indirect. L'emploi de la force a un caractère étatique indirect lorsqu'un Etat est impliqué de manière importante dans des actes non étatiques pratiqués par des pirates informatiques. La mise en place d'une préparation à la défense n'est pas contraire à l'interdiction du recours à la force*. *Les attaques de réseaux informatiques qui n'atteignent pas l'intensité d'un acte physique de violence armée, comme, par exemple, l'attaque du système informatique bancaire d'un pays, violent non pas l'interdiction du recours à la force, mais le principe de non-intervention.*

3.2.2. Droit de légitime défense

Le droit de légitime défense, individuelle ou collective, est réglé à l'art. 51 de la Charte des Nations Unies ; il a aussi la valeur d'une règle de droit coutumier. Mais pour qu'il soit licite de recourir à la force dans un cas de légitime défense, il faut que des conditions déterminées soient réunies. Ces conditions s'appliquent également à la réaction à l'emploi de la force armée commis via des réseaux informatiques.

3.2.2.1. Agression armée

La première condition à laquelle l'art. 51 de la Charte des Nations Unies subordonne le droit de légitime défense est la commission d'une agression armée. Mais, selon la jurisprudence de la CIJ, toute violation du principe du non-recours à la force n'a pas le caractère d'une agression armée[83]. Un Etat ne peut prétendre jouir d'un plein droit de légitime défense que si l'agression militaire dont il est l'objet atteint une certaine intensité. Si la violation du principe de non-recours à la force dont un Etat est victime reste en deçà du niveau d'intensité de l'agression armée, cet Etat a toutefois le droit de prendre immédiatement des mesures de défense proportionnées sans caractère militaire.

3.2.2.2. Principe de la proportionnalité

La proportionnalité des mesures de défense est un principe de base du droit de légitime défense. Même si une agression armée a été commise, les actes de défense doivent être proportionnés à l'agression subie pour être licites. On retrouve aussi ce principe de la proportionnalité en droit international humanitaire[84]. Toutefois, ce n'est pas la nature des armes employées mais leur effet qui est déterminant. Si l'attaque d'un réseau informatique a une intensité égale à une agression armée, les actes de légitime défense conduits en réaction à cette attaque peuvent en principe utiliser des armes de même nature ou de nature différente. Dans un cas comme dans l'autre, l'intensité des effets produits doit être conforme au principe de la proportionnalité. Si

[83] CIJ, "Activités militaires et paramilitaires au Nicaragua et contre celui-ci (Nicaragua v. Etats-Unis d'Amérique)", *C.I.J Recueil* 1986 , p. 104 : "Mais la Cour ne pense pas que la notion d' « agression armée » puisse recouvrir non seulement l'action de bandes armées dans le cas où cette action revêt une ampleur particulière, mais aussi une assistance logistique ou autre. On peut voir dans une telle assistance une menace ou un emploi de la force, ou l'équivalent d'une intervention dans les affaires intérieures ou extérieures d'autres Etats." Voir aussi p. 127. Opinion controversée dans la doctrine, cf. IPSEN (N. 67), p. 1087.

[84] Voir chiffre 3.4.

les actes de légitime défense dépassent les limites de la proportionnalité, ils violent alors à leur tour le principe du non-recours à la force.

3.2.2.3. La légitime défense préventive, une démarche controversée

A partir de quand le recours à la force constitue-t-il un cas de légitime défense ? C'est une question cruciale. En principe, il faut qu'une agression ait été commise pour que naisse le droit de légitime défense. Les opinions divergent quant à savoir si le droit de légitime défense naît également lorsqu'une agression armée est imminente (cas Caroline datant de 1837 : « *cases in which the necessity of self-defence is instant, overwhelming and leaving no choice of means, and no moment for deliberation* »). Le problème tient ici à la zone grise que constitue le terme « imminent », dont la définition résulte d'une décision individuelle de l'Etat agresseur qui est quasi invérifiable[85].
Néanmoins, compte tenu des armes et des menaces d'aujourd'hui, on peut difficilement demander à un Etat d'attendre d'être effectivement victime d'une agression avant d'entreprendre de se défendre. Mais pour prendre des mesures de défense militaires, il faut qu'il existe un danger grave et imminent dont l'existence est clairement vérifiable ; la simple aggravation d'une menace ou prévisibilité d'une agression ne suffit pas.

Le devancement de l'agression que constitue la légitime défense préventive mise en place par la doctrine américaine en 2002 sous le nom de « *preemptive strikes* » (frappes préventives) est contraire à la conception en vigueur en droit international public. Avant l'agression de l'Irak par les Etats-Unis en 2003, plusieurs membres du Conseil de sécurité ont répété qu'ils étaient opposés à cette extension du droit de légitime défense au domaine de la prévention. Il y a lieu de penser qu'à l'issue de la guerre en Irak, la majorité des Etats se rallieront à cette opposition.

3.2.2.4. Agression armée ayant un caractère étatique direct ou indirect

Pour avoir le droit de légitime défense, il faut que l'agression armée soit imputable à un Etat. Or, nous avons vu plus haut au sujet de l'emploi de la force qu'il peut être particulièrement difficile de retrouver la source des attaques de réseaux informatiques. On peut toutefois penser qu'une CNA s'inscrit dans une opération plus vaste, qu'il faudrait analyser avec précision si le cas se produisait.
La légitime défense est admise pour répondre également à l'exercice indirect de la force par un Etat si le niveau d'intensité de l'agression armée est atteint. Dans son arrêt Nicaragua, la CIJ a estimé que « l'envoi » de groupes armés « par un Etat ou sur mandat d'un Etat » constituait une agression armée si les actes commis par la force des armes avaient une ampleur et des conséquences dépassant le simple incident de frontière. En revanche, le simple fait de fournir des armes ou un soutien logistique à des rebelles ou à des bandes armées ne constituait pas, aux yeux de la Cour, une agression armée même s'il violait le principe du non-recours à la force. En conséquence, le simple fait qu'un Etat a formé des pirates informatiques qui exécutent une attaque armée au travers des réseaux informatiques ne serait pas suffisant pour conférer un plein droit de légitime défense contre cet Etat ; il faudrait qu'en outre les pirates agissent sur mandat de l'Etat qui les a formés.

Dans ce contexte, l'exercice de la force par des groupes terroristes pose un problème particulier lorsqu'il a des conséquences assimilables à une agression armée alors que les terroristes ne sont pas sous le contrôle de l'Etat d'où est parti l'agression. Dans le cas de l'attaque du 11 septembre 2001, le Conseil de sécurité a établi, dans sa résolution 1368, que les Etats-Unis avaient un droit de légitime défense individuelle et collective. Al Quaida n'était pas sous le contrôle du régime taliban ;

[85] Au sujet de la « zone grise », voir IPSEN (N. 67), p. 1089.

mais dans le cas de l'Afghanistan, des résolutions du Conseil de sécurité établissaient que le régime des Talibans soutenait l'organisation terroriste Al Quaida[86]. Selon la pratique des Etats et la jurisprudence de la CIJ, l'allégation qu'un autre Etat abrite ou soutient des terroristes, alors que le lien avec l'emploi de la force commis n'est pas prouvé, ne suffit pas pour faire valoir un droit de légitime défense[87].

3.2.2.5. Pas de représailles militaires

Le droit de légitime défense suppose en principe non seulement qu'une agression armée a eu lieu (ou qu'elle est imminente dans le cas de la légitime défense préventive, cf. supra), mais aussi qu'elle est encore en cours. Il est illicite de conduire des représailles armées pour sanctionner une agression armée qui a eu lieu antérieurement mais qui n'est plus en cours.
Conclusion : *Pour qu'un Etat ait un droit de légitime défense en cas d'attaque contre ses réseaux informatiques, il faut que les conditions suivantes soient remplies cumulativement : 1) L'attaque au travers les réseaux informatiques doit avoir les mêmes conséquences qu'une agression armée physique. 2) Elle doit atteindre une certaine intensité. 3) Elle doit être imputable à un Etat, c'est-à-dire que les pirates informatiques doivent soit être des agents d'un Etat, soit agir sur mandat d'un Etat. 4) L'attaque doit avoir eu lieu et être encore en cours ou être imminente et inévitable. Si ces conditions sont remplies, l'Etat visé a le droit de légitime défense quelle que soit la nature des armes qu'il emploie, pour autant que le principe de la proportionnalité soit respecté. Si l'une de ces conditions n'est pas remplie, l'Etat ne bénéfice pas du droit de légitime défense individuelle ou collective prévu à l'art. 51 de la Charte des Nations Unies. Des options envisageables sont des mesures de sécurité collective ou une réaction étatique à la violation de l'interdiction d'intervention.*

3.2.3. Le système de sécurité collective des Nations Unies

Le système de sécurité collective des Nations Unies, qui est ancré au Chapitre VII de la Charte, est le corollaire essentiel de l'interdiction absolue du recours à la force. Globalement, la Charte prévoit que le droit de légitime défense peut être exercé seulement jusqu'à ce que le Conseil de sécurité ait pris lui-même des mesures. Toutefois, cette « primauté » des mesures du Conseil de sécurité sur le droit de légitime défense de l'Etat agressé est resté, jusqu'à ce jour, sans portée dans la pratique.

En cas d'attaque conduite via des réseaux informatiques, comment le Conseil de sécurité peut-il entrer en action ?

Selon l'art. 39 de la Charte des Nations Unies, le Conseil de sécurité peut prendre des mesures de contrainte à caractère non militaire et militaire dans l'une ou l'autre des trois situations suivantes : menace contre la paix, rupture de la paix ou acte d'agression.

Les attaques via des réseaux informatiques assimilés à un emploi de la force armée peuvent être considérées comme constituant une rupture de la paix ou un acte d'agression[88]. Le Conseil de sécurité a également la possibilité de prendre des mesures au titre du Chapitre VII de la Charte s'il constate l'existence d'une simple « menace contre la paix ». Dans ce cas, le Chapitre VII prévoit une gradation dans les mesures possibles, allant des sanctions non-militaires aux sanctions militaires. Le choix des mesures à prendre dans chaque cas d'espèce est laissé à la discrétion du

[86] RES 1214 (1998), RES 1257 (1999) ; voir la discussion à ce sujet dans IPSEN (N. 67), PETERS (N. 67) et BOTHE (N. 67).

[87] Voir aussi l'avis de la CIJ concernant le mur de sécurité : CIJ, "Conséquences juridiques de l'édification d'un mur dans le territoire palestinien occupé", Avis consultatif, *C.I.J. Recueil* 2004 ainsi que *Projets d'articles sur la responsabilité des Etats pour les faits internationalement illicites* (N. 72).

[88] Selon l'opinion dominante, la notion d'« acte d'agression » est comprise comme étant plus large que la notion d'« agression armée » au sens de l'art. 51 de la Charte des Nations Unies ; cf. PETERS (N. 67), p. 324.

Conseil de sécurité. Ainsi, lorsqu'il apparaît qu'une attaque via des réseaux informatiques peut difficilement être assimilée à un emploi de la force armée (p. ex. parce qu'elle porte sur le système de paiement, le système bancaire ou le système boursier d'un pays), le Conseil de sécurité peut néanmoins ordonner des mesures au titre du Chapitre VII de la Charte. Les compétences du Conseil de sécurité sont donc plus larges que le droit de légitime défense individuelle ou collective inscrit à l'art. 51 de la Charte.

Conclusion : *Le système de sécurité collective offre plus d'options pour réagir à une agression au travers des systèmes informatiques que le droit de légitime défense individuelle et collective prévu à l'art. 51 de la Charte des Nations Unies.*

3.3. Les CNO et l'interdiction d'intervention

La notion d'intervention se définit comme l'immixtion directe ou indirecte d'un Etat dans les affaires intérieures ou extérieures d'un autre Etat par l'utilisation de moyens coercitifs. Considérée comme une règle de droit coutumier, l'interdiction d'intervention découle *in fine* du principe de l'égalité souveraine des Etats inscrit à l'art. 2, al. 1, de la Charte des Nations Unies[89].

3.3.1. Contenu de l'interdiction d'intervention

Toute violation de l'interdiction de l'emploi de la violence est également une violation de l'interdiction d'intervention. L'interdiction d'intervention est en effet plus large que l'interdiction de l'emploi de la force puisqu'elle peut englober la contrainte économique, politique ou autre. Toutefois, la limite entre l'influence, qui est licite, et la contrainte, qui est interdite, ne peut pas être fixée en général, mais doit être établie sur la base d'une appréciation au cas par cas. Cela est particulièrement vrai de la contrainte économique. Le droit coutumier ne fonde pas de droit aux relations économiques internationales ou à l'aide économique. Néanmoins, on peut émettre l'hypothèse qu'une attaque informatique qui détruit le réseau bancaire d'un pays, par exemple, est une intervention illicite. Il est également difficile de dire où commence et où finit une « intervention subversive » dans le cas de la manipulation d'un contenu qui peut être effectuée via des réseaux informatiques.

Comme le principe du non-recours à la force, le principe de non-intervention peut être violé de manière indirecte. Les questions d'imputabilité de la violation en question se posent dans les mêmes termes que pour l'exercice indirect de la force et l'agression armée indirecte[90]. Dans ce cas également, l'Etat doit en principe être impliqué de manière importante dans l'intervention non étatique interdite. Une propagande subversive n'est en principe pas considérée comme une violation de l'interdiction d'intervention lorsque l'Etat depuis le territoire duquel cette propagande est diffusée la tolère sans pour autant en avoir le contrôle[91].

3.3.2. Réaction à des interventions interdites

Les CNA associées à l'exercice d'une contrainte économique, comme par exemple la destruction de réseaux bancaires, sans pour autant atteindre le niveau d'intensité de l'agression armée ne permettent pas de faire valoir un plein droit de légitime défense individuelle ou collective.

Le droit international public donne plusieurs possibilités de défense à l'Etat qui subit des attaques informatiques de ce type. Selon l'art. 2, al. 3, de la Charte des Nations

[89] Au sujet de l'interdiction d'intervention, lire PETERS (N. 67) ; IPSEN (N. 67) ; KÄLIN (N. 67).

[90] Voir chiffre 3.2.2.4.

[91] JAAC 61 (1997), n° 129, p. 1030.

Unies, les Etats sont tenus de régler leurs différends par des moyens pacifiques. Cela comprend les démarches diplomatiques, la désignation de tribunaux arbitraux ou la saisine de la Cour internationale de justice à la Haye. Il est également possible que la communauté des Etats entre en action et que le Conseil de sécurité, constatant une « menace pour la paix », ordonne des mesures coercitives au titre du Chapitre VII de la Charte.

Enfin, le droit international public connaît les sanctions unilatérales, comme les mesures de rétorsion ou les représailles[92].

Une mesure de rétorsion est un acte inamical qui n'est pas contraire au droit international public en soi. On peut citer à titre d'exemple le refus de conclure un traité intéressant pour la partie adverse ou la rupture des relations diplomatiques. Traditionnellement, on estime qu'une mesure de rétorsion n'a pas besoin d'être proportionnée puisqu'elle ne contrevient pas au droit international public. Néanmoins, l'idée s'impose progressivement que le principe de la proportionnalité devrait être respecté dans ce domaine également.

Une mesure de représailles est un acte contraire en soi au droit international public, par lequel un Etat réagit au comportement d'un autre Etat également contraire au droit international public. Si elle est exécutée en réaction à un acte contraire au DIP, une mesure de représailles devient légitime. Mais pour qu'elle soit elle-même conforme au DIP, il faut que certaines conditions soient remplies : le principe de la proportionnalité doit être respecté et la partie adverse doit avoir été informée à l'avance des représailles qu'elle encourt. Le principe de la proportionnalité exige que les représailles ne soient pas mises en œuvre comme une « sanction », mais qu'elles aient pour but exclusif de restaurer une situation conforme au droit international public. En outre, les représailles ne doivent pas porter atteinte aux droits d'Etats tiers. Les avis divergent sur la question de savoir si un Etat doit avoir épuisé les moyens existants de régler le différend pacifiquement avant d'avoir le droit de recourir à des représailles. Traditionnellement, la Suisse a pour principe de s'engager en faveur du règlement pacifique des différends.

La rupture des relations économiques ou la pratique de discriminations dans les relations commerciales ne sont pas contraires en soi au DIP, pour autant qu'elles ne violent pas les règles de l'OMC ou les dispositions d'autres traités internationaux.

Conclusion : *Les attaques informatiques qui n'atteignent pas le niveau d'une agression armée physique, comme par exemple la destruction du système bancaire d'un Etat, sont contraires non pas à l'interdiction de l'emploi de la force, mais à l'interdiction d'intervention lorsque l'attaque est imputable à un Etat. L'Etat agressé ne peut pas utiliser la force militaire pour répondre. Il peut se défendre en prenant des mesures de sécurité collective ou en recourant à des moyens de règlement pacifique du différend. Les mesures de rétorsion et les représailles ne sont pas exclues, pour autant que l'attaque informatique soit imputable à un Etat et qu'elles respectent le principe de la proportionnalité.*

3.3.3. Les CNE et l'interdiction d'intervention

Reste la question de savoir si le simple fait qu'un organe étatique ou quelqu'un agissant sur mandat d'un Etat s'infiltre dans des réseaux informatique pour se procurer des informations est contraire au droit international public.

Dans ce domaine non plus, il n'y a pas de pratique des Etats ni de traité international.

[92] Lire à ce sujet PETERS (N. 67), IPSEN (N. 67).

L'analogie avec l'espionnage offre des pistes : dans la pratique des Etats, l'espionnage n'est presque jamais considéré comme contraire au droit international public. Les Etats ne réagissent généralement pas aux actes d'espionnage par des représailles, c'est-à-dire par des actes contraires au DIP, l'espionnage étant considéré comme un « acte inamical ».

Toutefois, la doctrine n'est pas unanime sur la question de savoir si l'espionnage constitue une violation de l'interdiction d'intervention au regard du droit international public[93]. En général, l'espionnage viole des dispositions du droit national des Etats ; de même, l'infiltration dans des réseaux informatiques de tiers est passible de poursuites pénales dans de nombreux Etats.

Le fait que le droit international public n'interdit pas l'espionnage en principe ne signifie cependant pas que les espions puissent invoquer le droit international public pour justifier leur activité s'ils font l'objet d'une procédure nationale[94].

L'un des problèmes posés par les CNE tient au fait que l'espionnage informatique ne requiert pas du tout la présence physique d'un « espion » sur le territoire – et donc dans l'espace judiciaire – de l'Etat visé. Le droit international public n'oblige pas à extrader les espions.

Conclusion : *Le droit international public n'interdit pas l'exploitation de réseaux informatiques (CNE). Par analogie avec l'espionnage, une opération dans un réseau informatique peut être qualifiée d'« acte inamical ». Cette qualification s'applique en principe à toute infiltration pratiquée dans des réseaux informatiques pour se procurer des informations, même si le but est de se renseigner sur les ressources adversaires basées sur les CND.*

3.4. CNO et *jus in bello*

Le droit international humanitaire ou *jus in bello*, qui s'applique uniquement aux conflits armés, remplit deux fonctions : il règlemente la conduite des hostilités et protège toutes les personnes qui ne participent pas ou ont cessé de participer aux combats. En revanche, il ne répond pas à la question de la licéité d'une guerre (*jus ad bellum*), question abordée plus haut. Le droit international humanitaire s'applique à tout conflit armé, que la participation à ce conflit soit « licite » ou non, et à toutes les parties au conflit.

Il est incontesté que le droit international humanitaire, avec l'ensemble de ses principes et règles, est applicable aussi aux actes d'agression commis via des réseaux informatiques dans le cadre d'un conflit armé[95]. Mais comme les attaques informatiques se distinguent des méthodes traditionnelles de guerre, l'application concrète du droit international humanitaire dans leur cas soulève toute une série de questions.

3.4.1. Les « attaques » selon le droit international humanitaire et les CNO

En droit international humanitaire, le terme d'« attaque » recouvre à la fois les actes d'agression et les mesures de défense. Il ne faut pas confondre la notion d'« attaque» en droit international humanitaire et la notion d'« agression armée » se-

[93] JOHN A. RADSAN : "The unresolved equation of espionage and international law", in *Michigan Journal of International Law*, p. 595-634.

[94] GRAF VITZHUM (N. 67), p. 143 s.

[95] International Expert Conference on Computer Network Attacks and the Applicability of International Humanitarian Law : Chairman's Conclusions, Stockholm, 17-19 novembre 2004 ; FALKO DITTMAR, Angriffe auf Computernetzwerke, Jus ad bellum und jus in bello, Berlin 2005 ; Michael N. Schmitt, CNA and The Jus in Bello : An Introduction (CNA), in Byström Karin, Proceedings of the International Expert Conference on Computer Attacks and the Applicability of International Humanitarian Law, Stockholm, Swedish National Defense College, 2004.

lon le *jus ad bellum*[96]. Selon l'art. 49, al. 1, du Protocole additionnel I aux Conventions de Genève[97], « *l'expression "attaques" s'entend des actes de violence contre l'adversaire, que ces actes soient offensifs ou défensifs*. » Par conséquent, lorsque le terme « attaque » est employé dans ce qui suit, il désigne à la fois les actes d'agression via des réseaux informatiques et les mesures de défense.

La définition de l'attaque au sens du droit international humanitaire porte moins sur l'action elle-même et les moyens employés pour l'exécuter que sur ses conséquences. On est en présence d'une attaque lorsqu'une action a des conséquences déterminées, comme des blessures ou la mort d'êtres humains, des dommages ou la destruction de biens matériels[98]. Les « attaques » informatiques ne peuvent donc être qualifiées d'attaques au sens du droit international humanitaire que si elles provoquent des blessures, des morts, des dommages ou des destructions. Les attaques de systèmes informatiques qui n'ont aucune des conséquences citées sont généralement licites au regard du droit international humanitaire.

3.4.2. Principes fondamentaux du droit international humanitaire

L'ensemble du droit international humanitaire codifié portant sur la conduite de la guerre (les quatre Conventions de Genève de 1949 et les deux Protocoles additionnels de 1977) ainsi que le droit international humanitaire coutumier sont applicables aux « attaques » informatiques. Il est utile de rappeler ici brièvement les principes fondamentaux du droit international humanitaire. Le non-respect de l'un ou l'autre de ces principes entraîne automatiquement une violation du droit international humanitaire.

3.4.2.1. Le principe de distinction

En vertu du principe de distinction, les belligérants sont tenus, en tout temps, de faire la distinction entre personnes ou biens civils et objectifs militaires (combattants et biens militaires) et de n'attaquer que les objectifs militaires. Ce principe, inscrit aux art. 48 et 51 du Protocole additionnel I, fait partie des règles essentielles du droit des conflits armés. Il recouvre trois catégories d'obligations : l'interdiction d'attaquer des personnes civiles[99] ; l'interdiction de diriger des « attaques » contre des biens civils ; et l'interdiction de mener des « attaques » sans discernement, causant des dommages civils collatéraux excessifs[100].

3.4.2.2. Le principe de précaution

Le principe de précaution est régi par l'art. 57 du Protocole additionnel I (Précautions dans l'attaque). De cette norme découlent différents devoirs pour les belligérants. Ils doivent veiller constamment à épargner les personnes et les biens civils et préparer les « attaques » de manière précise afin que les actions de guerre se déroulent comme prévu. Les parties à un conflit sont tenues en particulier d'annuler ou d'interrompre une attaque lorsqu'il apparaît que son objectif n'est pas militaire ou que le principe de la proportionnalité n'est pas respecté.

3.4.2.3. Le principe de la proportionnalité

Le but de la guerre est de mettre hors de combat l'adversaire et de le contraindre à la reddition en causant le moins possible de dommages à des personnes et à des

[96] Voir chiffre 3.2.2.1.

[97] RS 0.518.521.

[98] Cf. SCHMITT (N. 68), p. 112-113 ss.

[99] Cette règle ne s'applique cependant pas lorsque des personnes civiles participent directement à des hostilités et lorsque des biens civils sont utilisés à des fins militaires.

[100] Cf. ROBERT KOLB, Jus in bello, Le droit international des conflits armés : Précis, Bâle 2003, p. 115.

biens civils[101]. Le principe de la proportionnalité tient compte du fait que les « attaques » menées contre des objectifs militaires peuvent causer des dommages à la population civile et aux biens civils (dommages collatéraux)[102]. Ce principe oblige l'attaquant à « *s'abstenir de lancer une attaque dont on peut attendre qu'elle cause incidemment des pertes en vies humaines dans la population civile, des blessures aux personnes civiles, des dommages aux biens de caractère civil, ou une combinaison de ces pertes et dommages, qui seraient excessifs par rapport à l'avantage militaire concret et direct attendu* »[103]. Les belligérants sont donc tenus de choisir des moyens et des méthodes qui soient en rapport avec l'avantage militaire attendu. Pour qu'une « attaque » soit proportionnée, il faut qu'elle soit adéquate, nécessaire et raisonnable par rapport à l'objectif visé : elle est adéquate si elle permet d'atteindre l'objectif ; elle est nécessaire si aucune autre mesure également adaptée mais moins lourde ne permet d'atteindre l'objectif visé ; et elle est raisonnable si le rapport entre l'« attaque » et l'objectif visé est convenable.

3.4.3. Questions choisies concernant les CNO

Comme les « attaques » informatiques constituent une méthode de guerre nouvelle, différente des méthodes traditionnelles, de nombreuses questions concernant l'application du droit international humanitaire à ces « attaques » sont encore en suspens. Cela fait peu de temps que des groupes d'experts, composés de juristes et d'informaticiens, tentent de trouver des réponses à ces questions[104]. Il n'existe d'ailleurs pas encore de pratique bien établie des Etats à ce sujet.

Les paragraphes qui suivent font brièvement le tour des différentes questions que soulèvent les « attaques » de réseaux informatiques. Il s'agit, sans entrer dans tous les détails, d'illustrer les problèmes qui se posent de prime abord au regard des trois principes fondamentaux du droit international humanitaire.

Un premier problème tient au fait que les opérations dans les réseaux informatiques se caractérisent par l'utilisation de codes, de virus, de vers, de bombes logiques, etc. qui se propagent automatiquement. Ces virus peuvent se répandre dans des réseaux informatiques sans faire de distinction entre objectifs militaires et personnes ou biens civils, échappant au contrôle des personnes conduisant les attaques. Le danger existe donc que des « attaques » informatiques ne respectent pas le principe de distinction[105].

Ce principe est également violé lorsqu'il est impossible, lors d'une « attaque », d'opérer une distinction claire entre systèmes militaires et systèmes civils. Il y a souvent des interdépendances entre les uns et les autres : l'armée est de plus en plus tributaire des systèmes civils, par exemple pour les télécommunications[106].

Une autre caractéristique des « attaques » informatiques est qu'elles sont menées à distance. Cet aspect pose deux problèmes importants, susceptibles de se traduire en particulier par une violation du principe de précaution. Premièrement, la distance par rapport à l'objectif visé peut conduire à prendre pour cible un objet qui, en réalité,

[101] Cf. KOLB (N. 94), p. 58.

[102] Cf. DITTMAR (N. 68), p. 247 s.

[103] Art. 5, al. 2, let. a, ch. iii, Protocole additionnel I.

[104] Une conférence internationale d'experts a été organisée à Stockholm du 17 au 19 novembre 2004 dans le but d'ouvrir la discussion sur les CNA et les CND. Lors de cette conférence, il a été établi que le droit international humanitaire s'appliquait également aux « attaques » contre des réseaux informatiques. Plusieurs problèmes liés à cette nouvelle méthode de guerre ont en outre été identifiés. Pour plus de détails, voir chiffre 4.2.

[105] Cf. DAVIS BROWN, A Proposal for an International Convention To Regulate the Use of Information Systems in Armed Conflict, Harvard International Law Journal, vol. 47, n° 1, 2006, p. 22.

[106] Cf. DITTMAR (N. 68), p. 242.

n'est pas un objectif militaire. Deuxièmement, il est extrêmement difficile de remonter à la source de la première frappe si bien que la riposte risque d'être dirigée vers le mauvais objectif.

Dans la mesure où il est difficile de respecter les principes de distinction et de précaution dans les « attaques » informatiques, le respect du principe de la proportionnalité pose lui aussi problème. Les « attaques » de réseaux informatiques peuvent déclencher en cascade des effets qui touchent à la fois des biens militaires et des biens civils et dont l'ampleur peut être difficile à prévoir.

Les « attaques » de réseaux informatiques soulèvent ainsi un autre problème : la personne qui conduit les attaques a-t-elle concrètement la possibilité technique de séparer les réseaux militaires des réseaux civils, d'identifier avec précision la cible de l'« attaque » et d'éviter les effets en cascade afin de garantir le respect des trois principes fondamentaux du droit international humanitaire ?

La question du statut des personnes impliquées dans une action de combat pose également un problème particulier. Concrètement, il s'agit de déterminer si l'action conduite par une personne civile doit être qualifiée de participation directe aux hostilités. Comme nous l'avons dit, les attaques de réseaux informatiques peuvent être menées depuis un point géographiquement très éloigné de la cible. La personne qui exécute l'attaque peut ne pas être un membre des forces armées, mais un informaticien spécialisé. Cette personne peut même être basée dans un pays qui n'est pas partie au conflit. L'exécution d'une attaque constitue une participation directe aux hostilités. Mais comment faut-il qualifier l'entretien du système utilisé pour conduire des attaques ou les mesures de sécurité prises pour défendre ce système contre les attaques ? Et comment peut-on agir contre une personne civile qui, en raison de sa participation à des hostilités, a perdu la protection dont elle bénéficie contre les attaques directes, en particulier si elle se trouve dans un pays tiers ?

Cette bref tout d'horizon illustre la nécessité de procéder à une analyse complète des questions techniques et pratiques avant d'entamer une analyse juridique des modalités à suivre pour respecter les principes et les règles du droit international humanitaire dans le cadre des CNO.

Conclusion : *Le droit international humanitaire est applicable en principe aux actions de combat menées via des réseaux informatiques. Toutefois, un grand nombre de questions juridiques restent ouvertes. Pour leur apporter une réponse, il faut d'abord procéder à une analyse complète des aspects techniques et pratiques..*

3.5. Les CNO et le droit de la neutralité

Pour la Suisse, il est particulièrement intéressant de savoir quelles sont les questions que les CNO posent au regard du droit de la neutralité.

Le droit de la neutralité s'applique lorsqu'un conflit armé oppose des Etats. Si des mesures militaires ont été décidées par le Conseil de sécurité, le droit de la neutralité ne s'applique pas car ses fondements résident dans le droit de la guerre classique.

A titre préalable, il importe de rappeler le devoir fondamental de l'Etat neutre de ne pas violer le principe du non-recours à la force[107].

3.5.1. Le territoire de l'Etat neutre

Si un conflit armé oppose des Etats, l'Etat neutre a le devoir de ne pas mettre son territoire à la disposition des belligérants. Il a également le devoir de défendre ce ter-

[107] Voir chiffre 3.2.1.

ritoire. Inversement, les belligérants sont tenus de respecter l'inviolabilité territoriale de l'Etat neutre.

Ces droits et devoirs territoriaux de l'Etat neutre soulèvent quelques questions dans le cas des CNO. Si le cyberespace était considéré comme un espace appartenant en propre à un Etat, comme par exemple l'espace aérien, cela aurait pour conséquence que l'Etat neutre serait tenu de bloquer l'accès des belligérants à ses réseaux informatiques et, inversement, que les belligérants devraient renoncer à faire un usage abusif de ces réseaux.

Mais contrairement aux avions, les données ne sont pas pilotées lorsqu'elles sont acheminées vers leur objectif. Souvent, on ne peut même pas déterminer quel chemin prennent les données échangées internationalement. S'il est possible de fermer un espace aérien à des aéronefs spécifiques, cela est beaucoup moins évident pour des données dans un réseau informatique. En outre, une partie des données passent par des satellites, qui se trouvent dans l'espace et donc hors du champ d'application du droit de la neutralité.

Pour toutes ces raisons, on estime généralement que l'espace virtuel constitué par le cyberespace n'est pas assujetti à la règle qui veut que l'Etat neutre interdise son territoire aux belligérants. Inversement, les belligérants ne violent pas le droit de la neutralité lorsque des données passent par des réseaux informatiques neutres lors d'actions de combat[108].

La conclusion que l'Etat neutre n'est pas tenu de fermer ses réseaux de données aux belligérants en cas de guerre découle également, par transposition, de l'art. 8 de la Convention de La Haye, selon lequel « une Puissance neutre n'est pas tenue d'interdire ou de restreindre l'usage, pour les belligérants, des câbles télégraphiques ou téléphoniques, ainsi que des appareils de télégraphie sans fil, qui sont, soit sa propriété, soit celle de compagnies ou de particuliers. »[109]

Le droit de la neutralité implique cependant une limite à l'usage d'armes causant des dommages sur un territoire étendu[110]. Le territoire de l'Etat neutre doit être épargné par les possibles effets secondaires des actions de combat. Il est donc en principe interdit aux belligérants d'infliger des dommages aux réseaux informatiques des Etats neutres par des actions de combat menées via des réseaux informatiques.

3.5.2. Absence de soutien des belligérants par l'Etat

Un Etat neutre n'a pas le droit de soutenir des belligérants, que ce soit au moyen de troupes ou d'armes. Si l'on transpose cette interdiction aux CNO militaires menées dans le cadre de conflits armés, cela signifie qu'un Etat neutre ne peut pas consentir à ce que les belligérants utilisent ses réseaux militaires. En principe, les réseaux militaires sont protégés et ne sont donc pas accessibles au public.

Conclusion : *En cas de conflit entre Etats, l'Etat neutre n'est pas tenu de bloquer l'accès aux réseaux de données accessibles au public afin que les belligérants ne puissent les utiliser abusivement pour commettre des attaques informatiques. Les réseaux militaires, en revanche, ne doivent pas être mis à la disposition des belligérants et doivent donc pouvoir être protégés*

[108] Voir aussi DITTMAR (N. 68), p. 263 ss.

[109] RS 0.515.21.

[110] Voir aussi BOTHE (N. 67), p. 714.

4. Tendances internationales

4.1. Convention du Conseil de l'Europe sur la cybercriminalité

Si l'on prend en considération le domaine d'application matériel de la convention, force est de constater que celui-ci n'exclut pas les opérations militaires. C'est pourquoi les CNO devront à l'avenir être aussi analysées à l'aune de la Convention du Conseil de l'Europe de 2001 sur la cybercriminalité.

La Convention du Conseil de l'Europe sur la cybercriminalité du 23 novembre 2001, entrée en vigueur le 1er juillet 2004, est la première convention internationale – et jusqu'à ce jour la seule – qui traite de la criminalité informatique et des infractions contre les réseaux informatiques. Elle oblige les Etats contractants à adapter leur législation pénale ainsi que les dispositions relatives à l'entraide internationale en matière pénale aux dernières innovations technologiques dans le domaine de l'information. A cet égard, cette convention ne met pas directement en question les CNO mais pose plutôt les conditions de base que doit respecter le droit pénal interne.

La convention renferme dans sa première section des dispositions de droit pénal matériel destinées à harmoniser cette matière entre les Etats. Ce sont en particulier les articles 2 à 6 (accès illégal, interception illégale, atteinte à l'intégrité des données, atteinte à l'intégrité du système, abus de dispositifs) qui intéressent les CNO et en particulier l'art. 2 (accès illégal). L'art. 143bis CP a manifestement été complété dans cette optique d'harmonisation[111]. La deuxième section de la convention introduit des règles applicables à la procédure pénale et traite des problèmes liés à l'administration et à la conservation de données informatiques ayant valeur de preuves pour l'instruction pénale. La dernière section de la convention a pour objet l'entraide internationale en matière pénale entre les Etats. Il importe en effet que la collaboration entre les parties contractantes se déroule de manière rapide et efficace.

La Suisse a signé la convention le 23 novembre 2001. La procédure de consultation relative à son approbation et à sa mise en œuvre devrait s'ouvrir dans les premiers mois de l'année 2009.

4.2. Violation du droit international public humanitaire par les CNO

A l'issue de la 28ème Conférence internationale de la Croix-Rouge et du Croissant-Rouge, la Suisse, la Suède et la Finlande ont promis de lancer un processus international en vue d'examiner l'applicabilité du droit international humanitaire aux attaques informatiques[112]. Une première réunion internationale d'experts organisée par la Suède s'est tenue en décembre 2004. A cette occasion, les experts sont arrivés à la conclusion que les CNO n'étaient pas illicites en soi, mais que certaines d'entre elles pourraient cependant représenter une violation du droit international humanitaire[113].

[111] La teneur de cette disposition est la suivante:

Art. 143bis Accès indu à un système informatique

Celui qui, sans dessein d'enrichissement, se sera introduit sans droit, au moyen d'un dispositif de transmission de données, dans un système informatique appartenant à autrui et spécialement protégé contre tout accès de sa part, sera, sur plainte, puni d'une peine privative de liberté de trois ans au plus ou d'une peine pécuniaire.

[112] Cf. aussi THOMAS C. WINGFIELD, When is a Cyber Attack an "Armed Attack?" Legal Thresholds for Distinguishing Military Activities in Cyberspace, The Potomac Institute for Policy Studies, 2006.

[113] Voir ch. 3.4.

Dans le prolongement de ces débats sur la question, la Suisse a récemment proposé d'organiser à son tour une nouvelle réunion d'experts[114].

5. Réponses aux questions posées le 17 octobre 2007 par la DélCdG

Question 1: les bases légales existantes sont-elles suffisantes pour autoriser la défense de réseaux informatiques? – Selon notre définition de CND non-agressive, les bases légales existantes sont suffisantes.

Question 2: quelles sont les bases légales qui autorisent les services du DDPS à procéder à des CNE et à des CNA ? Dans le cadre de quels genres d'engagements de l'armée peut-on faire appel à des CNE et à des CNA? – Le recours à des CNE et à des CNA n'est possible qu'en cas de service actif. Il n'existe pas de bases légales pour les autres types d'engagements. Nous sommes d'avis que le recours à des CNA ne peut avoir lieu qu'en cas de service actif, de sorte qu'une base légale formelle n'est pas nécessaire. Une base légale formelle est en revanche nécessaire pour procéder à des CNE.

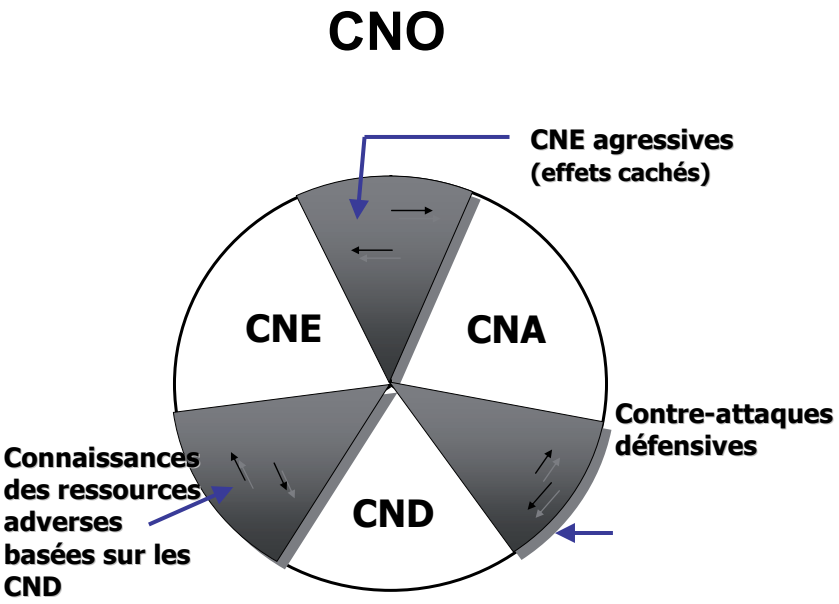
Question 3: qu'en est-il des bases légales existantes applicables au service de renseignements (art. 99 LAAM) par rapport à celles qui pourraient régir les InfoOps de l'armée, en particulier la recherche des informations par le biais de CNE? – La base légale existante applicable au service de renseignements (art. 99 LAAM) n'autorise pas la recherche d'information par le biais de CNE.

Question 4: quelles conséquences aurait l'adoption du nouvel art. 18m LMSI (perquisition secrète d'un système informatique) sur les opérations de CNE et de CNA entreprises par le DDPS? – L'adoption du nouvel art. 18m LMSI (perquisition secrète d'un système informatique) n'aurait aucune incidence sur les opérations de CNE et de CNA menées par le DDPS, attendu que cette disposition ne s'applique qu'au service de renseignements compétent.

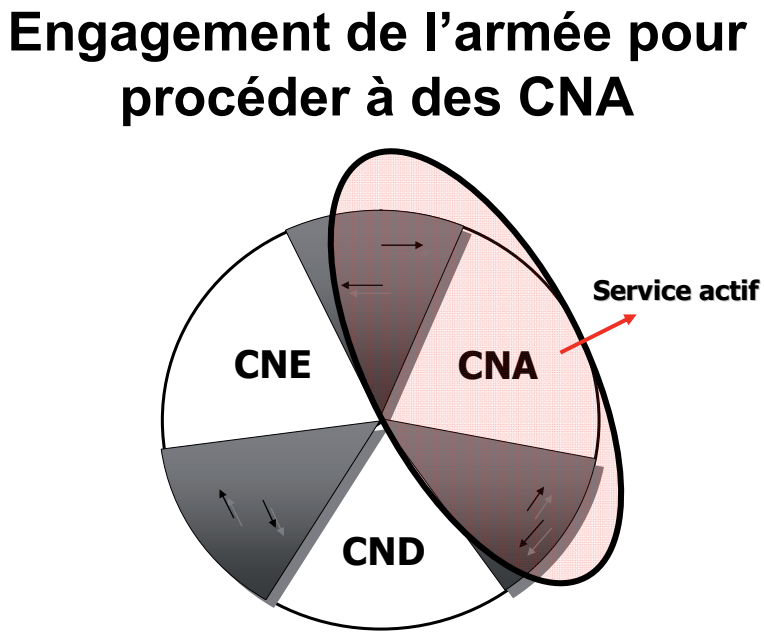
[114] Rapport de politique étrangère du 15 juin 2007, FF 5257, 5313 s.

Annexe

Graphique 1

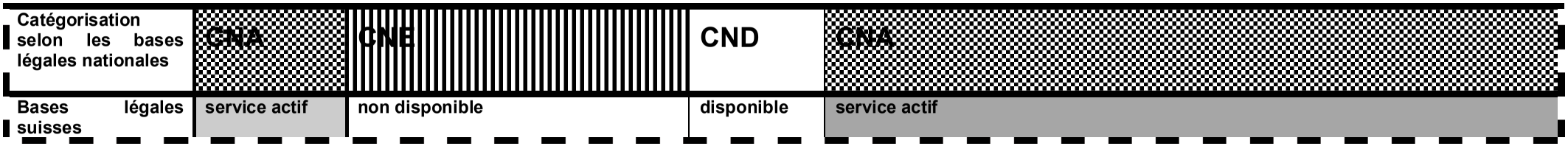


Graphique 2



Graphique 3

	CNE + (CNE agress.) **Mise en place des effets cachés pour préparer une attaque possible**	**CNE *stricto sensu*** **Infiltration dans des systèmes informatiques ou récolte d'informations par des effets cachés**	**CND +** (CND explorat.) **Connaissances des ressources adversaires basées sur les CND par infiltration dans des réseaux informatiques**	**CND *stricto sensu*** **Sécurité informatique**	**CND +** (CND off.) **Contre-attaques en réaction à des CNA de l'adversaire < du seuil d'agression armée selon l'art. 51 de la Charte des Nations Unies**	**CND +** (CND off.) **Contre-attaques en réaction à des CNA de l'adversaire > du seuil d'agression armée selon l'art. 51 de la Charte des Nations Unies**	**CNA *stricto sensu*** **Attaque contre des réseaux informatiques non assimilée à une agression armée**	**CNA *stricto sensu*** **Attaque contre des réseaux informatiques assimilée à une agression armée**
Jus ad bellum (***jus contra bellum***) **et droit international public général** *traité sous les points 3.2. et 3.3.*	interdit viole le principe du non-recours à la force *traité sous le point 3.2*	non interdit violation du principe de la non-intervention? *traité sous le point 3.3.3*	non interdit violation du principe de la non-intervention? *traité sous le point 3.3.3*	admis	admis, mais pas le recours à la force armée vaut pour les réactions à une violation directe ou indirecte du principe de la non-intervention, selon les règles de la responsabilité des Etats réaction préventive à un danger imminent ? *traité sous le point 3.3.*	admis, incl. le recours à la force armée vaut pour les réactions à une agression armée directe ou indirecte, selon les règles de la responsabilité des Etats réaction préventive à un danger imminent ? *traité sous le point 3.2*	non autorisé ne viole pas le principe du non-recours à la force, mais le principe de la non-intervention. vaut pour les interventions directes ou indirectes, selon les règles de responsabilité des Etats *traité sous le point 3.3.*	interdit viole le principe du non-recours à la force vaut pour des agressions armées directes ou indirectes, selon les règles de responsabilité des Etats *traité sous le point 3.2.*
Jus in bello **(droit international humanitaire)** *traité sous le point 3.4*	*s'applique, si les opérations sont pratiquées dans le cadre d'un conflit armé international ou interne selon les conventions de Genève*			non pertinent	*s'applique, si les opérations sont pratiquées dans le cadre d'un conflit armé international ou interne selon les conventions de Genève*			
Droit de la neutralité *traité sous le point 3.5*	*s'applique en cas de conflit interétatique*			non pertinent	*s'applique en cas de conflit interétatique*			


Catégorisation selon les bases légales nationales
CNA
CNE
CND
CNA
Bases légales suisses
service actif
non disponible
disponible
service actif