Le juste milieu

Prise de position sur la cybersécurité

La numérisation progresse à une vitesse fulgurante et concerne aussi bien la société civile que le monde politique et les milieux économiques. La numérisation offre de nombreuses possibilités, mais implique aussi de devoir relever des défis importants : la délocalisation des activités criminelles dans le cyberespace (mais aussi les cyberattaques entre États) soulignent de manière de plus en plus claire aux yeux du monde politique et de l'opinion publique la nécessité de sécuriser le cyberespace. Le PBD, parti du progrès, utilise depuis longtemps déjà les instruments modernes des technologies de l'information et de la communication (TIC). Véritable parti de la raison, le PBD est toutefois conscient des risques correspondants et défend donc aussi la sécurité de notre cyberespace. Par conséquent, il propose ce qui suit.

La cybersécurité, un problème mondial

La numérisation croissante de notre monde a ouvert des perspectives d'interconnexion au sein de la société civile et du monde économique qui étaient inimaginables il y a quelques décennies seulement. Le revers de ce phénomène du « monde qui devient un village » est son utilisation à des fins illicites. La numérisation a des effets positifs, mais aussi négatifs d'une ampleur jusqu'ici inconnue. L'utilisation illégale des technologies numériques est et sera l'un des défis majeurs du XXI^{e} siècle. Le cyberespace est de plus en plus utilisé pour des activités criminelles, des luttes de pouvoir politique et des activités de renseignement. Des cyberattaques d'infrastructures telles que l'approvisionnement électrique et les télécommunications via les réseaux numériques peuvent déstabiliser un pays tout entier. La numérisation ne s'arrête donc pas aux frontières, et ce phénomène global modifie en profondeur la politique internationale et soulève de nouveaux défis en politique extérieure et en politique de sécurité.

Les formes de conflits en particulier et les moyens utilisés dans ce cadre ont changé avec la numérisation. Compte tenu de l'évolution technique, le cyberespace est un nouveau terrain sur lequel les conflits se développent. Les moyens traditionnels utilisés lors de conflits sont seulement complétés par ces nouveaux instruments.

Jusqu'à il y a quelques années, la politique de sécurité mettait avant tout l'accent sur les criminels. La défense des intérêts nationaux par cyberattaque était alors peu connue et l'utilisation militaire des cyberarmes est elle aussi un phénomène relativement récent : la première attaque avérée de ce type s'est produite en 2011.

Le danger constitué par les cyberattaques est dû aux divers intervenants : il peut s'agir d'un individu ou de groupes de hackers professionnels, de bandes criminelles ou de commandos de hackers militaires ou des services de renseignement. Les équipes de hackers professionnelles et soutenues par un État sont aujourd'hui la plus grande source de danger

puisqu'elles se livrent à des activités d'espionnage (industriel) ou lancent des attaques sur des infrastructures critiques.

L'utilisation illégale du cyberespace est avant tout fondée sur le fait qu'il n'est nulle part ailleurs aussi facile de supprimer ses propres traces d'activités (criminelles). Il est donc difficile, voire impossible, d'attribuer de manière précise ces activités, particulièrement celles de nature agressive.

Une autre caractéristique de l'utilisation illégale des technologies numériques est l'effacement des frontières entre le civil et le militaire ; même les hackers gouvernementaux n'utilisent pas des moyens vraiment différents de ceux des cybercriminels « ordinaires ».

L'important est que le principe de territorialité est caduc, notamment pour les données numériques, lorsqu'elles sont déconnectées de leur source avant d'être traitées et enregistrées de manière globale. Il faut donc plutôt parler d'espace partagé. Le cyberespace n'est pas homogène et n'a pas de frontières juridiques clairement délimitées. Le cyberespace ne peut donc être appréhendé comme un espace traditionnel de politique de sécurité.

Une autre particularité du cyberespace est l'effacement de la frontière entre l'offensive et la défensive. Pour l'armée et les services de renseignement en particulier, il est dorénavant considéré que le fait de pénétrer dans un système informatique étranger et d'analyser ses faiblesses ne constitue pas une attaque au sens classique du terme.

Enfin, les terroristes grouillent aussi dans le cyberespace : actuellement, ils l'utilisent (encore) essentiellement à des fins de propagande. Dans le même temps, des réseaux sécurisés sur Internet sont utilisés pour planifier des attaques ou coordonner des cellules terroristes.

« Avec le cyberespace, l'être humain s'est pour la première fois donné un espace (virtuel) qu'il utilise maintenant pour ses luttes intestines. La cybersécurité est un intérêt fondamental de la prévoyance étatique, mais les mécanismes classiques de mise en œuvre issus du monde réel y échouent en grande partie. »[1]

Le problème non encore résolu de cet espace créé par l'être humain est le transfert des principes internationaux de l'espace analogique à l'espace numérique et leur application. Certes, plus de 70 États ont formulé des stratégies de cybersécurité, auxquelles s'ajoutent des accords internationaux. Toutefois, des initiatives à l'échelon international font défaut, par exemple des règles et un code de conduite des États sur les réseaux.

[1] http://www.bpb.de/apuz/235533/sicherheit-im-cyberspace?p=all, consulté le 8 octobre 2018

Le PBD demande donc que la Suisse défende plus activement à l'échelon international des règles claires pour les cyberactivités des États. En tant qu'espace virtuel, le cyberespace est soumis à d'autres lois, comme expliqué précédemment. Cependant, il y a lieu de s'assurer que nos principes de droit international sont aussi appliqués dans cet espace. La Suisse, État de taille modeste, en est tributaire.

La cybersécurité en Suisse

Bien que le problème de la cybersécurité soit en premier lieu un problème international (le cyberespace n'a que faire des principes de souveraineté nationale ou de territorialité), il faut aussi prendre des mesures à l'échelon national pour garantir un niveau de sécurité le plus élevé possible.

Ces dernières années, la Suisse a pris certaines mesures pour améliorer la sécurité du cyberespace. La Stratégie nationale de protection de la Suisse contre les cyberrisques (SNPC) de 2012 doit ainsi permettre à la Suisse d'identifier les menaces possibles, de réduire les cyberrisques et d'améliorer la capacité de résistance des infrastructures critiques. Il ne s'agit alors pas uniquement de procéder à une analyse des risques et de la vulnérabilité, mais d'investir dans la recherche et le développement et de définir une politique de gestion des crises. En 2018, le Conseil fédéral a adopté la nouvelle SNPC, fruit d'une collaboration entre la Confédération, les milieux économiques et les hautes écoles. Les mesures définies vont de la constitution de compétences et d'un savoir à des mesures de cyberdéfense par l'armée et les services de renseignement, en passant par la coopération pour la poursuite pénale de la cybercriminalité.

Sur la base de cette SNPC, des standards minimaux en lien avec les risques en matière d'information et de communication pour les entreprises suisses ont été développés en 2018 en collaboration avec les milieux économiques. Une centaine de consignes concrètes doivent aider les entreprises à améliorer leur capacité de résistance aux cyberrisques.

La Centrale d'enregistrement et d'analyse pour la sûreté de l'information MELANI est une pièce maîtresse du dispositif de défense. Elle a pour mission d'identifier au plus tôt les cyberrisques et d'épauler les exploitants des infrastructures importantes.

L'armée, cible possible de cyberattaques, se focalise quant à elle sur la défense de ses propres infrastructures. En outre, elle a établi un plan d'action Cyberdéfense qui doit être mis en œuvre d'ici 2020. Depuis 2018, l'armée suisse propose par ailleurs une cyber-école de recrues : il s'agit de former des spécialistes pour protéger dès 2020 les centres de calcul et systèmes de communication de l'armée contre d'éventuelles cyberattaques.

Le juste milieu

Enfin, le Conseil fédéral vise la création d'un centre de compétence en cybersécurité et d'un comité du Conseil fédéral sur la cybersécurité.

Malgré ces mesures, le PBD estime qu'il y a encore des lacunes qui doivent être comblées pour que la Suisse et ses infrastructures soient protégées le mieux possible des cyberattaques. Le PBD demande donc :

- **Une plus grande sensibilisation de la population aux problèmes de la cybercriminalité.**
- **L'adoption de la loi sur la sécurité de l'information. La Confédération est confrontée chaque jour à d'immenses volumes de données et d'informations qui doivent être protégées. Une loi sur la sécurité de l'information instaure des exigences minimales en matière de sécurité qui doivent être respectées par toutes les autorités.**
- **L'introduction d'un devoir d'annonce légal en cas d'incident menaçant la sécurité. Les exploitants d'infrastructures critiques doivent avoir l'obligation de signaler aux autorités les incidents en lien avec le cybersécurité.**
- **Le développement des capacités de MELANI pour l'avertissement précoce et le soutien en cas de cyberattaques graves.**
- **L'instauration de standards minimaux contraignants dans les secteurs d'activité critiques (par exemple l'approvisionnement énergétique).**
- **La promotion par la Confédération de la formation à la cybersécurité dans les hautes écoles, car la Confédération en particulier a besoin d'experts bien formés.**

<u>La cybersécurité, pour les entreprises suisses également</u>

La cybersécurité ne concerne pas seulement les infrastructures critiques ou l'armée, mais aussi les milieux économiques. Ce ne sont pas uniquement les grandes entreprises internationales qui sont visées par les cybercriminels, mais aussi et de plus en plus les PME. La cybercriminalité cible en effet ce qui peut rapporter gros pour un effort modeste, donc aussi les PME suisses. Celles qui ne se préoccupent pas des questions de sécurité et qui ne prennent pas de mesures de défense appropriées sont les premières visées.

Les activités criminelles vont du chantage au sabotage, en passant par le vol de données ou l'espionnage.

Selon une étude réalisée en 2017 auprès des PME suisses, près de 40% d'entre elles sont victimes de cyberattaques. Les entrepreneurs doivent donc penser comme dans le monde réel à la manière dont ils souhaitent protéger leur entreprise. Nombre d'entre eux ne peuvent toutefois réagir de manière adéquate aux menaces, faute de disposer du savoir correspondant.

Le juste milieu

Or, il ne faut souvent pas grand-chose pour améliorer nettement la sécurité d'une PME. Par exemple, réviser régulièrement les dispositifs de sécurité. Ou établir un concept de sécurité individuel, adapté à l'entreprise.

Le mot-clé en matière de cybersécurité dans les milieux économiques suisses est « responsabilité individuelle ». Chaque entreprise est responsable de sa propre sécurité, que ce soit dans le monde analogique ou le monde numérique. Des systèmes décentralisés et hétérogènes doivent être préférés à une réglementation centrale (étatique), ce d'autant plus que les entreprises ne sont pas toutes menacées de la même manière. Toutefois, les PME ne doivent pas être laissées seules à se débrouiller avec cette tâche. Il faut favoriser l'entraide. Le PBD demande donc :

- **La sensibilisation des entreprises suisses aux cyberrisques.**
- **La rédaction par les associations sectorielles suisses de lignes directrices indiquant aux entreprises concernées comment gérer les cyberrisques. Les entreprises doivent alors bénéficier des expériences réalisées par les grandes entreprises.**
- **La mise à disposition de possibilités de formation continue et de centres de consultation en matière de cybersécurité pour les PME.**

Force est de constater que les PME forment la colonne vertébrale de notre économie et celle-ci doit être protégée de toute activité criminelle, que ce soit sous forme analogique ou numérique. Car au final, protéger nos PME des cyberrisques revient à protéger nos emplois.