Construire la confiance dans le cyberespace : la diplomatie internationale au servie de la cyberstabilité

Autor(en): **Crespo, Laura**

Objekttyp: **Article**

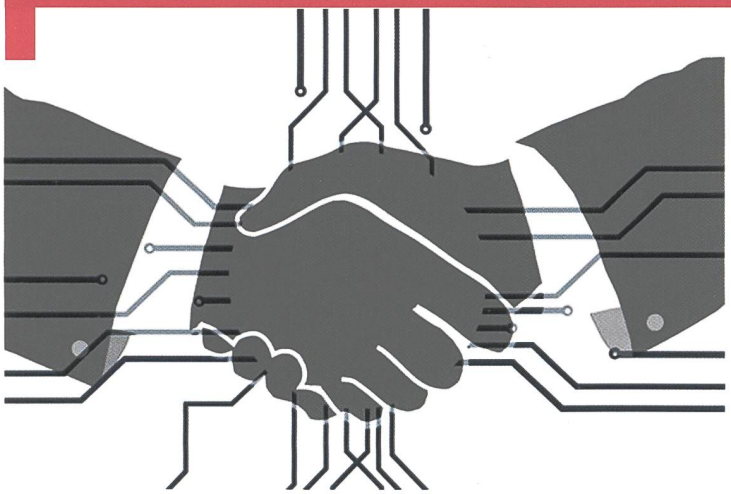
Zeitschrift: **Revue Militaire Suisse**

Band (Jahr): **- (2019)**

Heft 3

PDF erstellt am: **27.06.2024**

Persistenter Link: https://doi.org/10.5169/seals-867960



Cyber

Construire la confiance dans le cyberespace – la diplomatie internationale au service de la cyberstabilité

Laura Crespo
Cheffe suppléante, Bureau pour la politique étrangère et de sécurité au cyberespace, DFAE

La diplomatie est l'art de la négociation. C'est une forme de communication entre États qui a évolué déjà de nombreuses fois en raison du progrès technique. Pour les Etats, il s'agit de conduire des négociations et de trouver des compromis afin de vivre en paix les uns avec les autres.

Le cyberspace représente une nouvelle dimension de la communication entre Etats et, par conséquent, de la politique extérieure. Cela signifie que la cybersécurité est plus systématiquement prise en considération dans les réflexions de politique extérieure, entre autres parce que les économies sont de plus en plus interconnectées dans le cyberspace. Grâce aux technologies de l'information et de la communication (TIC), l'économie est plus innovante et compétitive au niveau international.

Cette compétitivité est extrêmement dépendante du bon fonctionnement des TIC. C'est donc dans l'intérêt de tous les Etats modernes, y compris de la Suisse, de protéger ses infrastructures et leurs utilisateurs des dangers inhérents, qu'ils soient de nature criminelle, politique ou terroriste.

L'objectif de la politique extérieure dans le cyberespace ?

Les cyberopérations visant l'Estonie en 2007, le conflit territorial russo-géorgien en 2008 et le virus Stuxnet en 2010 (déployé pour empêcher l'enrichissement de l'uranium iranien) ont tous servis à réveiller la communauté internationale et l'inciter à intégrer le domaine cyber dans ses efforts diplomatiques. Le manque de transparence et de prévisibilité perçu par les Etats en matière de TIC a été exacerbé par la nature immatérielle des voies numériques, le degré élevé d'anonymat et la possibilité de nier des activités dans le cyberespace. Cela montre clairement que la communauté internationale se meut dans un environnement politiquement instable, marqué par la méfiance et l'incertitude. Dernièrement, certains Etats ont été accusés publiquement d'avoir influencés les résultats des élections par l'intermédiaire du cyberespace, ce qui contextualise encore le climat géopolitique.

De manière générale, l'objectif de la cyberdiplomatie est de contribuer à un cyberespace ouvert, sûr et libre. En matière de politique de sécurité, cela signifie que le cyberespace doit être utilisé de manière pacifique et ne pas devenir un lieu où les Etats transposent leurs conflits, ni un lieu où les tensions entre Etats s'exacerbent.

Afin d'atteindre ce but, la confiance entre les Etats est une condition *sine qua non*. Dans un tel contexte, il est essentiel de créer de la confiance au sein de la communauté internationale et d'établir des voies de communication afin d'éviter l'éruption de conflits causée par des malentendus.

Les mesures de confiance – un outil adéquat pour le cyberespace ?

Les mesures de confiance sont apparues pour la première fois pendant la guerre froide avec pour objectif de répondre aux préoccupations militaires et en particulier le risque d'attaque «surprise». Bien qu'elles soient principalement axées sur la maîtrise des armements et le désarmement, elles ont progressivement évolué pour devenir des outils importants de gestion des crises. Dans les années qui ont suivi la fin de la guerre froide, ces mesures sont devenues un outil populaire dans le domaine de la gestion des conflits. En effet, les avantages qu'on pouvait en tirer semblaient inépuisables. Dès lors, les Etats ainsi que les organisations régionales et internationales ont eu recours à ces mesures pour instaurer la confiance, renforcer la coopération ainsi que réduire les risques de malentendus et d'escalade de la violence.

Récemment, les mesures de confiance sont devenues un élément central des discussions internationales sur la

sécurité du cyberespace. Depuis la fin des années 2000, l'Organisation pour la sécurité et la coopération en Europe (OSCE) a adopté des mesures de confiance visant à « réduire le risque de conflit découlant de l'utilisation malveillante des TIC ». Leur adoption a été précédée de négociations ardues et dans un contexte international qui n'était pas entièrement propice à la promotion et à l'instauration de la confiance.

Aujourd'hui plus que jamais, il est urgent de rehausser la barre de la confiance entre les Etats et de stimuler la coopération intra-étatique. Le Secrétaire général des Nations Unies a qualifié ce climat de « temps dangereux », soulignant l'importance de la confiance dans les programmes de désarmement entre autres dans le domaine nucléaire, de l'espace et du cyberespace.

Mesures de l'OSCE pour créer la confiance dans le cyberespace

En 2013 et 2016, les Etats participants de l'OSCE ont adopté un paquet de 16 mesures pour créer la confiance. Ce catalogue de mesures a trois objectifs : la transparence, la coopération et la stabilité. Concernant la transparence entre les Etats, elle est possible grâce à un échange systématique d'informations. C'est d'autant plus important dans le cyberespace qu'il y règne un haut degré de confidentialité de l'information.

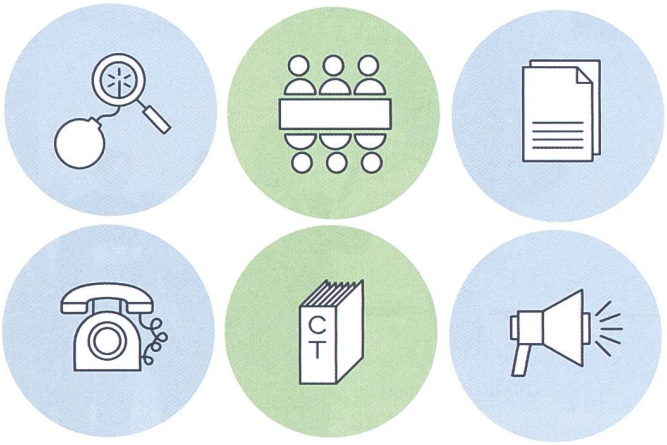
En outre, il est difficile de connaître les possibilités et les capacités cyber de chaque Etat, ce qui augmente la méfiance. Concernant la coopération, le catalogue prévoit de définir des interlocuteurs, des lignes de communication et des procédures à suivre en cas de crise afin d'éviter une escalade de la violence. Enfin, la stabilité consiste en des déclarations politiques visant à renoncer à attaquer des infrastructures critiques. Par cet accord volontaire et non contraignant au niveau politique, les 57 pays participants se sont déclarés prêts à échanger des informations concernant leurs institutions nationales, leurs perceptions concernant les menaces, leurs politiques et les mécanismes de coopération.

Conclusion

La confiance se construit progressivement. Les mesures de confiance tels que celles en cours au sein de l'OSCE peuvent contribuer à approfondir les relations interétatiques. Si certaines mesures de confiance répondent à des buts spécifiques, tel que la ligne directe de communication, l'objectif général du catalogue à long terme est de créer un dialogue perpétuel et évolutif.

Si certains progrès ont été accomplis dans l'adoption de ce catalogue, la volonté d'en appliquer les mesures et de limiter certains comportements malveillants ne vont pas de soi. En particulier, on pourrait attendre de la part des grandes puissances d'être exemplaire dans ce domaine afin de créer la stabilité.

Pourtant, l'environnement international actuel n'est pas entièrement propice à l'établissement ou au maintien de



la confiance entre les Etats. Les incidents constants en dessous du seuil d'un conflit armé exacerbent des relations interétatiques déjà tendues. Les failles systémiques de l'architecture mondiale des TIC fournissent aux adversaires (et parfois aux alliés) une source constante de possibilités pouvant être utilisée les uns contre les autres. En outre, les problèmes d'attribution de l'origine d'une action malveillante dans le cyberespace permettent aux auteurs d'en profiter. Les mesures de confiance et d'autres normes non contraignantes sont de plus en plus considérées comme insuffisantes pour limiter ces comportements. Cela a entraîné une hausse du seuil de conséquences pour les responsables d'activités malveillantes dans le cyberespace. Ces conséquences comprennent le fameux *shame & blame* ; à savoir la dénonciation et l'attribution publique et coordonnée, ainsi que l'adoption de mesures de rétorsion, bien que ces dernières fassent craindre d'autres représailles. Néanmoins, comme on l'a vu pendant la guerre froide, les moments de tension offrent d'immenses possibilités de coopération. Les dirigeants politiques et militaires ont alors compris l'intérêt des mesures de confiance, en tirant parti de celles-ci et en élargissant leurs champs d'application. A cet égard, le dilemme actuel n'est pas tant la nature ou le contenu des mesures de confiance que la qualité du *leadership* et de la vision politique.

L.C.