dation du programme réalisé à travers des tests et des analyses encore plus poussées tels que vérification (*model-checking* ou preuve). Il s'agit en fait de démontrer que le programme est correct, sûr, sécurisé. Le test est un métier bien établi, tandis que la vérification reste une tâche difficile, accessible aux chercheurs et aux ingénieurs du haut niveau (souvent ingénieurs docteurs). Nos ingénieurs diplômés maîtrisent le test (ce qui est normal), mais en plus ils ont de très bonnes notions de la vérification (ce qui constitue une compétence rare). Nous sommes persuadés que dans les années à venir les techniques de la vérification seront plus largement utilisées dans le domaine cyber, et nos ingénieurs pourront les utiliser.

Il s'agit de modèles, algorithmes et outils logiciels qui permettent la détection automatique des vulnérabilités des programmes ou la garantie « mathématiquement » de l'absence de vulnérabilités. Ce type de techniques a fait ses preuves, par exemple pour la validation des protocoles cryptographiques et même pour la recherche de virus, et nous prévoyons son adoption large par l'industrie dans les années à venir.

Une variante intéressante de cette technique, *runtime verification*, permettrait la détection automatique des attaques en cours en observant le comportement du système.

Conclusion

Pour conclure, il est clair que l'homme est un acteur majeur du cyberespace, et que les sciences humaines (psychologie, sociologie, droit, économie) ont un rôle important à jouer dans le domaine cyber. Donc l'exemple de l'EIDD montre que le curriculum d'une école d'ingénieurs universitaire fortement connectée aux SHS et à des laboratoires de physique et d'informatique de pointe a de grandes potentialités par rapport aux besoins d'aujourd'hui et de demain dans les domaines cyber industriel et militaire. Nous veillons à améliorer cette adéquation à travers les stages, et à travers les embauches dans ce secteur et au travers des interactions avec ses acteurs. En perspective il faudra mieux estimer les besoins en ingénieurs cyber et définir un référentiel de compétences – ce travail ambitieux et passionnant demandera la collaboration des nombreux acteurs du cyber.

"Existe-t-il un marché des cyber-armes ?" *Pour une approche critique de la notion de cyber-arme*

Aspirant Yves Auffret
Officier enseignant chercheur au Centre de Recherche de l'Armée de l'air (CReA).

Dépourvue d'une quelconque définition légale[1], ou d'un consensus de la doctrine, la notion de « cyber-arme » est difficile à définir. Ayant émergé dans le langage commun en 2010 avec l'affaire Stuxnet[2], elle demeure marginale dans la réflexion sur les cyberconflits.

Cette difficulté est accrue si on considère que la littérature scientifique se réfère au cyberespace en tant qu'arme. Les auteurs ont par ailleurs tendance à distinguer entre cyberattaque et cyberdéfense[3]. Par analogie, il est alors possible d'associer alors l'attaque à la notion d'arme. Mais c'est bien dans la littérature anglo-saxonne que la notion de cyber-arme est le plus souvent employée. Les « *cyberweapons* » y sont alors présentées comme, des outils informatiques de nature diverse opposés aux classiques *malwares*. Même présentes et identifiées, les analyses sur ces objets restent relativement rares.

Une fois ces problèmes de définition dépassés, le principe de l'existence d'un marché spécifique des cyberarmes et de sa dynamique apparaît d'autant plus problématique. Les développements suivants reprendront dès

1. La Loi n° 2013-1168 du 18 décembre 2013 relative à la programmation militaire pour les années 2014 à 2019 et portant diverses dispositions concernant la défense et la sécurité nationale fait référence à l'idée de « cybermenace » et ses apports juridiques sont dépourvus de références à des outils particuliers.
2. Marco De Falco, *Stuxnet Facts Report - A Technical and Strategic Analysis*, NATO CCD COE Publications, 2012.
3. Cf. Daniel Ventre, *Cyberattaque et cyberdéfense*. Paris, Hermès Publishing, 2011.

lors les hypothèses développées par Thomas Rid et par Peter McBurney[4]. Leur approche offre un cadre général et elle permet de traiter l'ensemble des logiciels malveillants sans établir de distinction artificielle entre la cyber-arme et le *malware*. L'enjeu de cette question n'est pas où acheter un virus informatique, mais bel et bien de savoir si ce type de logiciel dispose de caractéristiques facilitant la construction d'un cadre d'échange propice à sa prolifération en tant que cyber-arme.

D'autre part, derrière l'idée d'un marché des cyber-armes surgit l'idée de la prolifération de celles-ci. Or la définition proposée par ces deux auteurs s'avère assez restrictive. Elle conduit à conclure que le nombre des cyber-armes telles que Stuxnet auront vocation de par leurs coûts de développement et de mise en œuvre à demeurer des exceptions plutôt qu'une tendance. Ce constat tend à questionner finalement l'avenir d'un marché dédié aux cyber-armes. En outre, la confrontation de cette définition avec le concept de marché, replacé dans le contexte général du cyberconflit, viendra dévoiler un certain nombre d'interrogations et de faiblesses de la notion même de cyber-arme. De nos jours, le « marché cyber » peut tout être, sauf un marché de la cyber-arme.

La cyber-arme : de quoi s'agit-il ?

L'expression cyber-arme peut recouvrir deux logiques complémentaires : D'une part, elle peut permettre d'envisager l'outil technique et le moyen déterminant le caractère cybernétique d'une attaque. D'autre part, elle aurait vocation à englober l'ensemble des moyens techniques, matériels et humains dédiés aux cyber-attaques. C'est ainsi que la cyber-arme incarne au choix un ensemble détaillé de logiciels précis, ou le champ cyber dans son ensemble. Dans le premier cas, adopter le point de vue de la cyber-arme revient à restreindre très fortement l'analyse. Dans le second cas, la notion de cyber-arme n'a tout simplement plus aucun intérêt.

Réfutant la notion de cyber-guerre qu'ils jugent inappropriée, Thomas Rid et Peter McBurney défendent l'idée d'une cyber-arme qui dépasse la seule composante cyber d'un conflit. Ce choix les conduit à la première solution , et à une conception très restrictive : le « *weaponised software* ». Si une arme désigne tout outil conçu pour menacer ou pour causer des

4. Thomas Rid & Peter McBurney, "Cyberweapons", *The RUSI Journal*, Volume 157, Issue 1, 2012.

dommages physiques, fonctionnels ou psychologiques à des structures, des systèmes ou des êtres vivants, alors la cyber-arme est simplement le code informatique utilisé pour des objectifs identiques[5].

Le niveau technique et donc le niveau de puissance de ces « cyber-armes » fournit alors un critère pour une première typologie :

- les armes dites à faible potentiel, génériques, peu discrètes et d'acquisition facile, faciles à mettre en place et à contrer[6] ;
- les armes à fort potentiel, spécifiques, nécessitant des investissements lourds[7] ;
- les armes combinant des caractéristiques de ces deux catégories[8].

Dans la conception de ces armes, l'accroissement du potentiel destructeur induit deux efforts : d'une part, au niveau des ressources (Temps/Recherche/Investissement) ; d'autre part, au niveau du ciblage. Ces efforts participent à la réduction du nombre des dommages collatéraux potentiels de l'arme, réduisant également son pouvoir de coercition et de menace. Tout en sachant qu'une cyber-arme dispose d'une durée limitée pour agir avant que les défenses n'évoluent suffisamment pour la contrer.

L'exploitation des bugs et l'espionnage par l'intermédiaires des chevaux de Troie ne sont pas regardées comme des cyber-armes car moins dangereux[9] ; ils appelleraient des sanctions juridiques différentes.

Le coût prohibitif des cyber-armes à fort potentiel entraîne la diminution de leur risque de prolifération, comme n'importe quel autre sys-

5. "*For the purposes of this article, a cyber-weapon is seen as a subset of weapons more generally : as computer code that is used, or designed to be used, with the aim of threatening or causing physical, functional, or mental harm to structures, systems, or living beings.*" *Thomas Rid & Peter McBurney*, « *Cyberweapons* », ibid.

6. Les logiciels permettant les attaques de déni de service (DDoS) par exemple ; les attaques de 2007 en Estonie sont classées dans cette catégorie.

7. Notamment Stuxnet, Flame ou Gauss.

8. Certaines intrusions particulières, par exemple avec le virus I love you.

9. L'utilisation d'un mail piégé à l'aide d'un cheval de Troie ne serait donc pas considérée comme relevant d'une cyber-arme. *A fortiori*, l'ingénierie sociale et plus généralement les outils d'acquisition d'informations semblent ici exclus des utilisations premières de la cyber-arme. Le domaine d'une cyber-arme, du point de vue de la guerre de l'information, se limiterait paradoxalement à la dégradation des systèmes avec une variation dans le potentiel de dégâts en fonction du type d'arme en cause.

tème d'arme. De plus en raison du degré de précision (penser pour une cible identifiée voire unique), la cyber-arme dans son acception la plus restrictive devient difficilement « exportable ». De manière connexe, ceci tend à remettre en cause le postulat de la prééminence de l'attaque sur la défense dans le champ cyber. La défense est davantage présentée sous un jour favorable en raison de son coût moindre, donc de sa plus grande vitesse d'évolution.

Construite notamment sur le constat d'une absence de définition dans la doctrine américaine[10], cette approche s'avère intéressante pour différentes raisons.

Premièrement, face à une définition politisée et discutée de ce qu'est et de ce que doit être le cyberespace, il faut ici saluer l'effort qui consiste à vouloir réintégrer une forme de granularité technologique dans le raisonnement. Si on doit garder une vision normative de la définition proposée ici, il faut cependant considérer que cette granularité se construit en opposition avec l'idée de neutralité technologique qui conditionne la viabilité et la durabilité d'une norme par rapport aux évolutions de l'état de la technique. Si la notion de cyber-arme reste assez floue pour permettre une certaine interopérabilité dans la désignation, il faut mettre en avant sa spécificité.

Deuxièmement, en voulant s'affranchir de la cyber-guerre, Thomas Rid et Peter McBurney excluent de leur paradigme la question de l'acteur. On retrouve bien l'intention de nuire et la perception de la menace comme conditions de l'action ou encore l'effet psychologique sur la cible. Toutefois, ce sont ici des considérations qui semblent secondaires pour les auteurs. La question de la cyber-arme ne se pose pas en vertu de l'identité ou de la nature des acteurs. Corolairement, la cyber-arme n'est donc pas obligatoirement régalienne.

Enfin, on assiste à un paradoxe : d'un côté ce renoncement à l'acteur s'inscrit théoriquement dans les conceptions stratégiques qui font de la multiplication du nombre d'attaques un produit de la densification

10. « *Remarkably, even the US Department of Defense Dictionary of Military and Associated Terms, an authoritative 550-page compendium that defines anything from abort to Zulu time, has no definition for weapon, let alone for cyber-weapon* » Thomas Rid & Peter McBurney, op-cit.

DR

DR

et de la complexification des réseaux. De l'autre côté, le recours à une cyber-arme ne peut s'inscrire que dans un intérêt bien précis. Il s'agit de l'idée d'une émergence de cyber-attaques raisonnées et pensées comme une réalité dont les objectifs peuvent être économiques, idéologiques et/ou militaires. Les intérêts conditionnent ainsi paradoxalement la cyber-arme indépendamment (semble-t-il) de leurs propriétaires réduits à des propensions marginales.

Ainsi, adopter une approche restrictive de la cyber-arme conduit à décrire un ensemble précis et déterminé de logiciels malveillants. Cependant, cet ensemble qui n'est pas neutre est incapable de traduire la cyberattaque dans toute sa complexité et dans sa variété, et ignore les questions de l'exploitation des failles, du mécanisme de défense et des acteurs. De fait, la cyber-arme est un point de vue inefficace qui conduira à exclure la prise en compte de l'intégralité des marchés les plus fleurissants du secteur, notamment le marché global des technologies de sécurité informatique ou encore le marché des failles et de leurs codes d'exploitation.

Un marché des cyber-armes au prix de nombreuses exclusions.

Cet effort de définition est parmi les plus aboutis en ce qui concerne la cyber-arme. Toutefois, il ne peut être regardé comme suffisant pour répondre à la question de savoir s'il existe un marché des cyber-armes. Plus encore, il s'avère un obstacle à cette démarche. Car si le marché se conçoit comme un cadre de rencontre entre l'offre et la demande, plusieurs interrogations demeurent en suspens quand à l'intérêt et à l'organisation d'une telle structure pour les cyber-armes ainsi désignées. La grande question que l'on peut se poser est celle du secteur à considérer et de ses subdivisions (à inclure ou à exclure). Enfin, le caractère transparent de l'acteur dans la définition de la cyber-arme ne permettra pas de trancher la question du statut légal par essence de ce type de marché. Indépendamment de la confidentialité intuitive autour de ces échanges, il est impossible de savoir si nous avons à faire à un marché gris ou noir, sans se plonger dans la question de l'acteur qui devra faire l'objet de développements à part...

Pris dans l'idée d'une arme à faible potentiel, le marché est déjà existant depuis 1986/87 puisqu'il s'agit du marché des virus (et des antivirus) ; lequel est connu de tous et facilement accessible, y compris pour n'importe quel particulier. Notre idée du marché des cyber-armes passerait donc

nécessairement par le marché du virus informatique à l'exclusion des chevaux de Troie, des spywares ainsi que des virus « zombificateurs » qui sont hors de la définition. Il faut également exclure les équipements et les logiciels destinées à la protection des systèmes d'information ; nous touchons ici également, une des limites de cette définition de la cyber-arme ; elle ne prend pas en compte les moyens de se prémunir des attaques[11].

Il nous faut exclure également les logiciels de chiffrement ainsi que des outils qui permettent de se dissimuler, au-delà du marché des logiciels viraux et des technologies de sécurité entendues globalement. Comme le bug n'est pas regardé comme une cyber-arme, un autre domaine est à exclure malgré son caractère lucratif : le marché des vulnérabilités et de leurs codes d'exploitation[12]. Des failles, comme par exemple Heartbleed, ne pourraient être incluses dans le marché de la cyber-arme. La réponse à cette première interrogation tient donc dans l'idée que si l'arme à faible potentiel peut s'inscrire dans le marché des technologies de sécurité, elle ne peut caractériser l'essence d'un marché spécifique des cyber-armes à elle seule à cause des nombreuses exclusions opérées. Par ailleurs, la question initiale perd ainsi totalement de son intérêt. Le phénomène cyber ne serait porteur d'aucune originalité.

Pour répondre à cette question de l'existence d'un marché des cyber-armes de manière utile, il faudrait que la définition permette de dégager un nouveau marché uniquement dédié aux armes à fort potentiel. Et si un marché des cyber-armes existe avec toutes les restrictions évoquées, d'autres interrogations émergent notamment sur l'objet et sur le moment de l'échange. L'échange entre les acteurs de ce marché intervient-il au moment de la création de la cyber-arme ou de sa mise en œuvre ? Autrement dit, le marché de la cyber-arme est-il un marché de services ou un marché de biens ? Dans le premier cas, l'acheteur cherche des compétences afin de bâtir une cyber-arme qui serve ses objectifs tandis que le vendeur dispose de ces compétences. Dans le second cas, l'acheteur recherche une solution « clef-en-main » tandis que le vendeur propose des cyber-armes prêtes à l'emploi. Ce second cas correspondrait davantage au logiques d'une arme à faible po-

11. Le marché global des technologies de sécurité informatique était de 14,8 milliards d'euros en 2013,

12. Le marché des failles inconnues et des codes permettant de les exploiter (0-day exploit) produit environ 85 failles inconnues par jour, une faille Windows inédite pourrait ainsi se vendre jusqu'à 250.000 $ voir notamment : Pierluigi Paganini, « Zero-Day Exploits in the Dark », *Infosec Institute*, 21 avril 2015. http://resources.infosecinstitute.com/zero-day-exploits-in-the-dark/

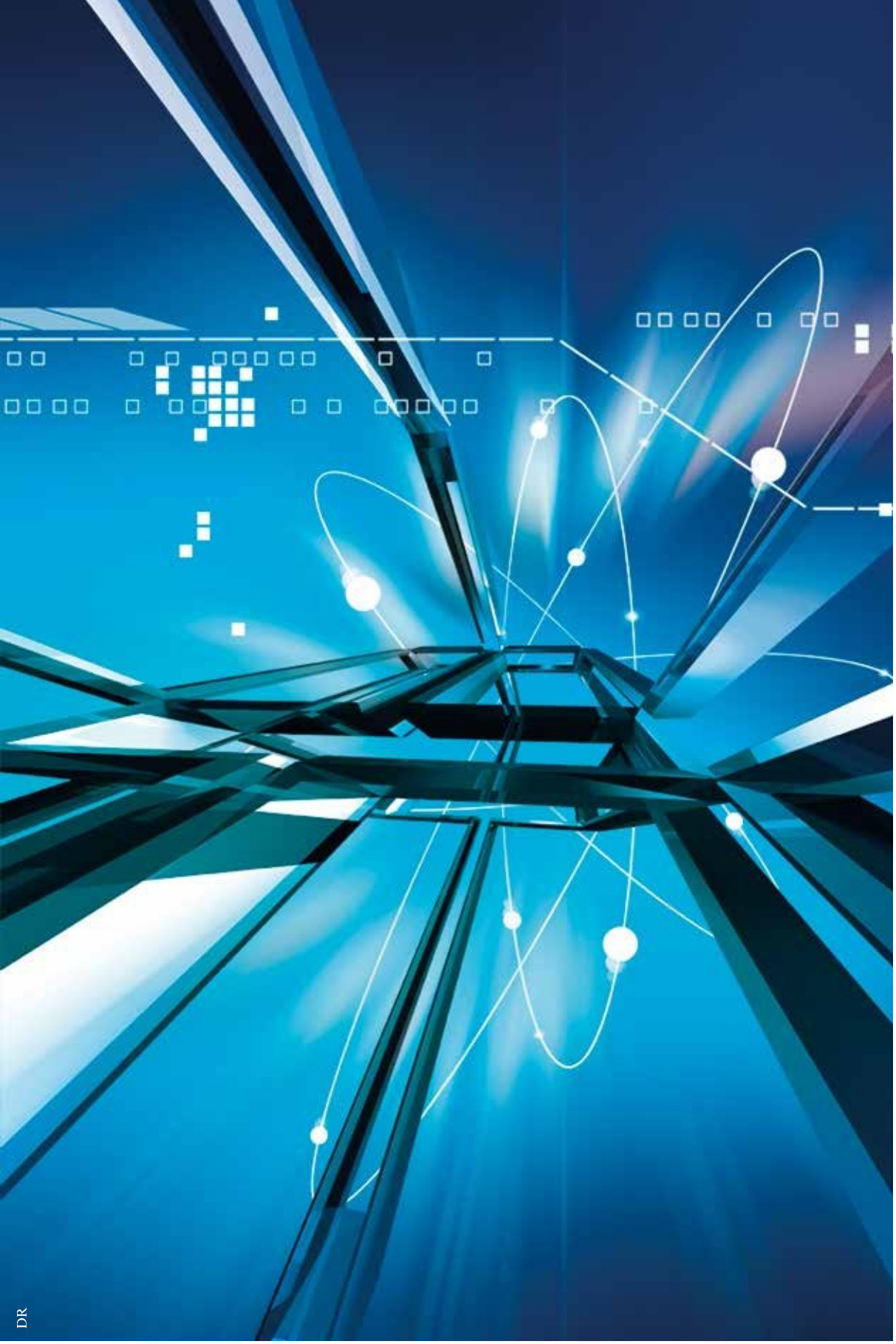
tentiel. Autrement-dit, compte-tenu des contraintes d'élaboration de l'arme, l'hypothèse d'un marché uniquement dédié aux cyber-armes à fort potentiel ne peut être qu'un cadre d'échange pour les compétences utiles ou/et des services entre un vendeur dépositaire de savoir-faire et un acheteur animé par un intérêt extrêmement précis (au sens qu'il ne peut trouver satisfaction sur les autres marchés du secteur). Le marché du travail existe bel et bien dans le champ cyber, seulement ce n'est pas un marché spécifiquement dédié à la conception de cyber-armes à haut potentiel...

Conclusion

Le marché de la cyber-arme ne peut ainsi exister sans englober le marché cyber dans son ensemble. Le risque de prolifération de la cyber-arme est limité par les importantes contraintes qu'elle impose à son utilisateur en matière de conception et d'emploi. En l'effet, les cyber-armes à faible potentiel disposent de marchés déjà connus. La question de l'existence d'un marché de cyber-arme trouve alors un intérêt inexistant. L'hypothèse d'un marché des cyber-armes à haut potentiel fondé sur l'échange de savoir faire destiné à la construction de ces mêmes armes ne peut se réaliser qu'au travers d'un ensemble plus vaste qui n'est pas spécifique en incluant des produits, et des services qui ne peuvent être regardés comme des cyber-armes.

Ainsi, bien qu'elle ne soit pas sans intérêt, la notion de cyber-arme ne peut servir à justifier de l'existence d'un seul et unique marché dédié. La prise en compte de la définition de la cyber-arme, ainsi que des exclusions auxquelles elle conduit, amène par ailleurs à replacer le risque par rapport aux autres risques du secteur. Car, il existe enfin plusieurs marchés sur lesquels ne s'échangent pas de cyber-armes mais des produits qui peuvent s'avérer tout aussi dangereux, voire causer bien plus de dommages (vulnérabilités, trojans...). Cette question conduit donc à nuancer le caractère terrifiant d'une cyber-arme à haut potentiel.

Au-delà de la question du marché, penser la question du risque au travers de la notion de cyber-arme est de nature à induire une erreur dans l'évaluation de ce dernier. Cette hypothèse pose tout simplement la question de l'utilité de cette notion. Une défense efficace ne peut se concevoir sous l'angle de la cyber-arme.



DR