Innovative Lösungen zum Schutz der kritischen IT-Infrastruktur

Christian Bühlmann Dipl. Inf.-Ing. EPFL

Zusammenfassung

Die Ereignisse des „11. September“ haben, sowohl auf Regierungsebene als auch in der Wirtschaft, zu einer Neubeurteilung der Sicherheitslage geführt. In diesem Zusammenhang ist die besonders anfällige Infrastruktur der Informatik (Energieversorgung, Datenleitungen, Telekommunikation) noch kritischer.

Der Autor untersucht auch aus strategischer Sicht verschiedene Faktoren wie zeitliche Abläufe, nicht voraussehbare Ereignisse usw., die gesamthaft zu einem bedrohlichen Überraschungseffekt eskalieren können.

Die Infrastruktur für die Informatik wird damit zu einem gefährdeten Knotenpunkt, wo bereits kleine Störungen grosse Auswirkungen verursachen können. Im heutigen Informatikumfeld kann aber damit die Regierungsfähigkeit oder die Führung der Wirtschaft enorm beeinträchtigt werden.

Nachdem der Autor das Umfeld der Technologie gezeigt hat, präsentiert er neue, auf künstlicher Intelligenz basierende Lösungen, die erlauben, Angriffe auf die kritische IT-Infrastruktur aufzudecken und abzuwehren.

Adresse des Autors:

Siemens Schweiz AG
Civil and National Security
Freilagerstrasse 40
CH-8047 Zürich
Security-info@siemens.com

Informationstechnik und Armee
42. Folge 2002/2003

1 Introduction

1.1 Argument

Les événements tragiques du 11 septembre 2001 obligent à repenser le risque et à prendre conscience de sa nouvelle réalité :
La victoire américaine dans la Guerre du Golfe en 1991 a montré aux adversaires potentiels des USA la futilité de s'y attaquer de manière symétrique. La même réflexion est valable pour tous les pays industrialisés. Les adversaires potentiels ou les organisations terroristes ont tiré les leçons de cet affrontement et recherchent désormais des stratégies indirectes.
La nouvelle menace est dissymétrique, voire asymétrique. Elle frappe là où nous sommes faibles et où nous ne l'attendons pas.
Corollaire de ce constat, la technologie est détournée pour devenir une arme. Le stratagème chinois « *Tuer avec une épée d'emprunt*[1] » est appliqué au pied de la lettre.
Ce genre de danger n'est pas nouveau, mais il prend une dimension jusque-là inconnue parce que la technologie moderne, étendue et omniprésente, peut être utilisée comme levier.
Nous affirmons ainsi que la technologie de l'information peut servir à la fois d'arme et de cible :

- **D'arme**, car la prise d'influence de systèmes de traitement de données permet de créer des effets similaires à ceux crées par l'emploi de la force.
- **De cible**, car la dépendance croissante de notre société vis-à-vis de l'infrastructure d'informatique critique fait que sa mise hors service, même partielle, a des effets certains sur la vie publique et économique.

Nous nous proposons de chercher à comprendre le mécanisme de la menace (en particulier dans ses aspects temporels), de rechercher sa nature et ses buts possibles, pour finalement proposer des solutions innovatrices.

1.2 Thèses

Sur la base de ce qui précède, nous avançons les quatre thèses suivantes :

- La maîtrise du facteur temps est la condition préalable du succès. La surprise est atteinte par la symétrie ou la dissymétrie.
- La menace a perdu son caractère symétrique et extérieure. Elle est interne et / ou dissymétrique.
- L'infrastructure d'information critique représente un centre de gravité stratégique.
- Au vu de ce qui précède, les solutions de protection classiques doivent être complétées par des systèmes innovateurs.

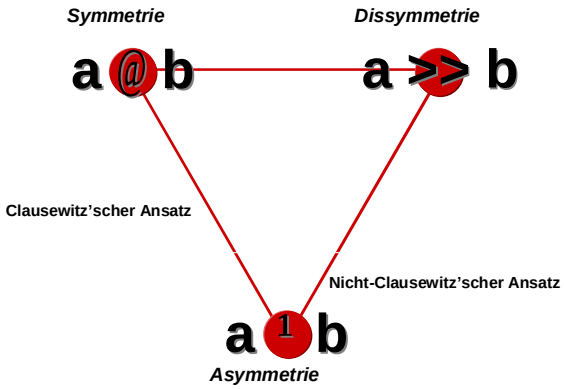

Figure 1 : Symétrie, dissymétrie, asymétrie.

[1] Cf. Anon, *Les 36 stratagèmes Traité secret de stratégie chinoise*, traduits et commentés par François Kircher, Editions Jean-Claude Lattès, 1991, ISBN 2-7096-0 987-8, pp. 38-43.

1.3 Corrélation entre moyens et finalité

La distinction classique entre symétrie et asymétrie est par trop simple et ne permet pas de cerner la problématique des disparités entre moyens et finalités.

En se basant sur les réflexions menées pas Siemens Suisse dans le cadre d'une étude sur l'art opératif, nous postulons que les finalités, perspectives et moyens des parties en conflit peuvent être du même ordre ou être, dans l'ensemble ou pour certains de ces objets, différents.

Il en va de même de leurs déterminations[2] réciproques à mettre les moyens en action.

Dans le premier cas, il y aura **symétrie** (des finalités, perspectives, moyens et/ou déterminations), dans le second **asymétrie** ou **dissymétrie**[3] (des finalités, perspectives, moyens et/ou déterminations).

- On observe un **conflit symétrique** lorsque les deux adversaires sont de force équivalente et qu'ils utilisent des moyens et des perspectives similaires pour atteindre une finalité analogue avec une détermination comparable. C'est le cas du duel, d'une lutte entre nations-états ou, au niveau tactique, entre deux forces terrestres ou deux forces aériennes.
- On parle de **conflit dissymétrique** lorsqu'il y a divergence au niveau des perspectives (doctrine) ou moyens (structures, importance, technologie ou équipements), mais que les finalités restent globalement semblables. C'est le cas du combat de David contre Goliath : David utilise le mouvement et le jet, Goliath, la protection de son armure et le choc de son épée.
- Dans le cas d'un **conflit asymétrique**, il y a une différence avant tout dans la finalité du conflit qui diverge entre les parties. C'est le cas des conflits entre puissances et petits états ou groupements non-étatiques, entre une composante terrestre et une guérilla. Les conflits asymétriques visent à atteindre des buts politiques sans moyens militaires. C'est avant tout la détermination de l'adversaire qui est visée par des engagements prolongés et de faible intensité.

Si les conflits symétriques sont par essence des guerres, les conflits asymétriques et dissymétriques ont lieu dans les cas de guerre, de crise ou de paix.

Ce modèle permet aussi de poursuivre la réflexion au delà du le cadre clausewitzien, dans lequel l'emploi de la force est subordonné à l'atteinte d'un but politique : *« [der] Krieg [ist] nichts (…)als die fortgesetzte Staatspolitik mit anderen Mitteln »*.[4] Les actions symétriques et dissymétriques ont lieu dans ce contexte. Les actions asymétriques ne sont pas forcément subordonnées à une finalité militaire et sortent du cadre usuel de l'opposition guerre / paix.

2 Le temps : le nerf de la guerre

L'engagement de la force a lieu de manière classique dans l'espace et le temps. Dans notre monde globalisé, où les frontières perdent en importance et où les informations sont disponibles en quasi temps-réel, l'espace perd de l'importance : *«Face à des situations ouvertes, le temps redevient la première dimension de l'action, bien davantage que l'espace"*.[5]

En se plaçant du point de vue de la menace, on peut se demander comment gagner la guerre ou l'engagement. Nous proposons deux pistes : la surprise et la rapidité de commandement.

---

[2] *Détermination* au sens de *volonté*.

[3] *Dissymétrie* : absence ou défaut de symétrie ; *Asymétrie* : absence de symétrie. Nous avons choisi dissymétrique en relation avec la doctrine française.

[4] Clausewitz, Carl von, *De la guerre*, traduction intégrale par Denise Naville, Paris :Les éditions de Minuit, 1955, ISBN 2-7073-0107-8, L I, chapitre I, page 51.

[5] Alain Minc, *La vengeance des nations,* Grasset, 1990, ISBN 2246440718**,** p. 245.

- La surprise « *découle en pratique des idées antithétiques de différer la détection et d'accélérer le contact*. »[6] Que ce soit au niveau opératif ou tactique, on observe une approche à couvert suivie d'un choc violent, brutal qui mène à la décision contre un adversaire stupéfié.
- Le processus de commandement, qui transforme les informations en ordres et en conduit la réalisation, est généralement modélisé par la **boucle OODA**, développée par le col John Boyd.[7]
  En simplifiant à l'extrême ses réflexions, on peut arguer que le processus de commandement forme un cycle de quatre phases : [8]
  - **O**bservation ;
  - **O**rientation ;
  - **D**écision ;
  - **A**ction.

  Boyd affirme que le succès est atteint lorsque les itérations de notre propre boucle OODA sont plus rapides que celles de l'adversaire, voire lorsque nous sommes capables d'influencer la boucle OODA adverse.[9]

2.1 Symétrie, asymétrie et dissymétrie appliquées au temps

Les aspects liés à la boucle OODA peuvent être exprimés dans le cadre des modalités exprimées ci-dessus.
Il s'agit de comparer les boucles OODA de deux parties en présence. Nous désignerons par **tempo** la rapidité de transition de la boucle OODA.
Le tempo relatif de deux parties peut ainsi être dans une relation de:[10]

1. **Synchronicité** : Les deux parties planifient et agissent dans les mêmes délais.
2. **Dissynchronicité** : Une partie conduit plus rapidement que l'autre et a un avantage clair puisqu'elle peut agir avant que son adversaire ait pu réagir. C'est, par exemple, le cas d'une armée disposant d'une conduite informatique et l'autre d'une conduite traditionnelle, à l'instar des forces coalisées et des forces iraquiennes lors de l'opération « Desert Storm » en 1991.
3. **Asynchronicité** : Le tempo de rouge est tellement lent que bleu ne remarque sa montée en puissance que trop tard. Il y a asymétrie, car rouge a une finalité dans la durée, alors que bleu aura vraisemblablement modifié sa finalité initiale. Au niveau stratégique, c'est l'approche terroriste du 11 septembre 2001. Au niveau tactique, c'est l'implémentation de la thèse de Leonhard.

---

[6] „*(...) Surprise (...) is brought about in practice by the antithetical ideas of delaying detection and hastening contact*." Leonhard, Robert R., *Fighting by Minutes Time and the art of war*, Praeger Publishers, 1994, ISBN 027594736X p. 141.

[7] John Boyd (1927 –1997), était un pilote de chasse de *l'US Air Force*. Voir Hammond, Grant T., *The Mind Of War, John Boyd and American security*, Washington and London : Smithsonian Institution Press, 2001, ISBN 1-56098-941-6 et Coram, Robert, *Boyd : The Fighter who changed the art of war*, Little, Brown and Company, 2002, ISBN 0-316-88146-5 ainsi que le site internet : http://www.belisarius.com, qui contient une version électronique des documents de Boyd cités ci-dessous [05.02.03].

[8] Boyd, John, *Destruction and Creation*, unpublished essay, Sept. 1976; *Pattern of Conflicts*, *A Discourse on Winning and Loosing*, 1995. La version finale de la boucle OODA (in « *The Essence in Winning and Loosing* ») a une connotation philosophique, voire théologique puisqu'elle "*illustrates the keys to life itself and the way in which one loses in its many competitions*" (Hammond, *op. cit*, p. 189).

[9] „*In order to win, we should operate at a faster tempo or rhythm than our adversaries or, better yet, get inside [the] adversary's Observation-Orientation-Decision-Action cycle or loop* ". Boyd, *Patterns of Conflicts*, Page 5.

[10] L'auteur assume la responsabilité pleine et entière de l'utilisation de ces néologismes qui n'ont pas reçu l'aval de l'Académie.

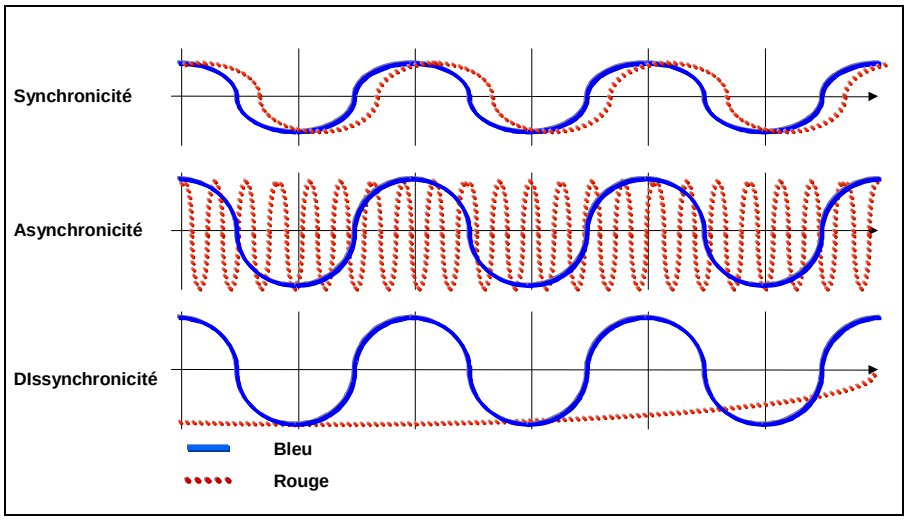

Figure 3 : Relations de symétrie dans le temps.

2.2 Problématique de la détectabilité

Pour la partie attaquée, le cas le plus délicat est celui de l'asynchronicité car l'attaque n'est détectée que trop tard. L'idée de réduire le seuil de détectabilité est délicate, car, à partir d'une certaine limite, on détecte aussi le bruit rémanent et le nombre de fausses alarmes explose. Le risque connexe du déluge de l'information doit aussi être relevé. Cette problématique, encore plus cruciale lorsque l'on ne sait pas exactement à quelle genre d'attaque on peut s'attendre, est à l'origine des couacs du renseignements, comme ceux relevés après les attaques terroristes.

2.3 Exemples

Les trois figures représentent les trois types d'attaques à base de synchronicité, dissynchronie ou asynchronie intégrant les deux paradigmes énoncés plus haut.

- L'attaque synchrone (Figure 3) est détectée et, comme bleu a une boucle OODA aussi rapide que rouge, il peut contre-attaquer.

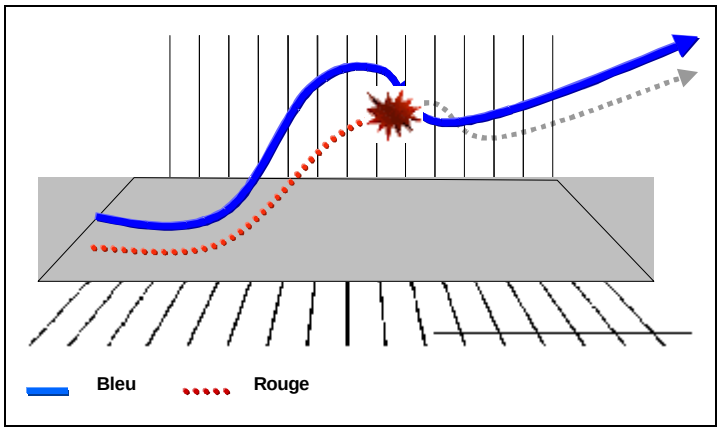

Figure 3 : Ataque synchrone.

- L'attaque dissynchrone est également détectée mais, comme la boucle OODA de bleu est moins rapide que celle de rouge, il est défait.

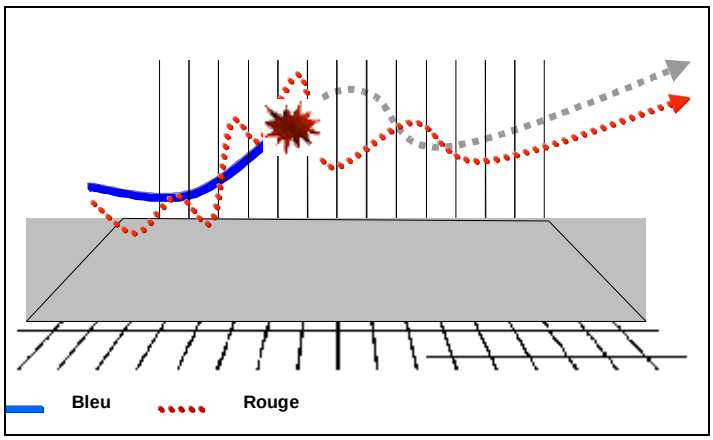

Figure 4 : Attaque dissynchrone.

- L'approche de l'attaque asynchrone a lieu sous le seuil de détection. La boucle OODA de bleu est mise en échec car la fonction « Observe » (le premier O de la boucle) ne peut pas détecter les préparatifs de rouge.

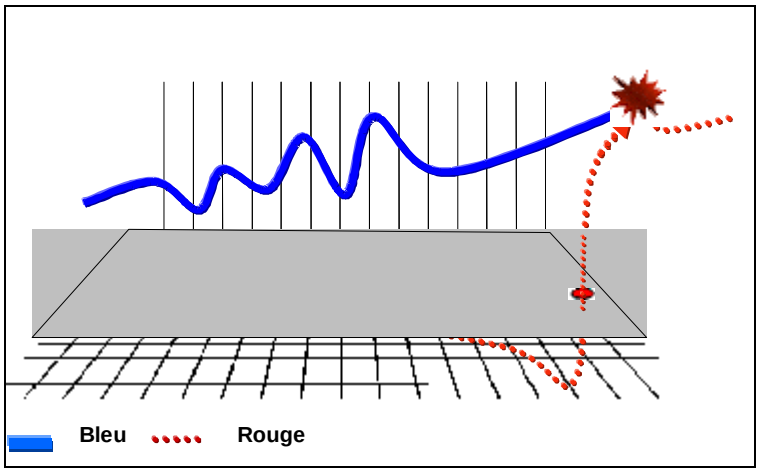

Figure 5 : Attaque asynchrone.

2.4 Justification de la première thèse

On voit clairement la forme que pourrait prendre une menace non symétrique pour atteindre au succès : l'application d'une asymétrie ou d'une dissymétrie dans le domaine temporel lui permet de créer la surprise et l'avantage par un changement de tempo oscillant de la lenteur à la rapidité.
En d'autres termes : « *C'est le temps qui fait la musique* ».

3 La menace : interne et asymétrique

Hors du domaine sécuritaire classique (militaire, police), nous découvrons chaque jours de nouvelles failles dans la sécurité de nos sociétés, en particulier dans le domaine de la sécurité de l'information. Ainsi, de manière exemplaire, la dernière semaine de janvier 2003 a été marquée par l'apparition du ver *SQL Slammer* qui a considérablement ralenti le transfert des données sur l'Internet.[11]

---

[11] Voir par exemple, une description grand public dans Schenker, Jennifer L., *Look Out! Inside the PC ! It's the killer worm*, Time, Europe, February 10, 2003, pp. 68 – 69 ou http://www.robertgraham.com/journal/030126-sqlslammer.html pour une analyse plus détaillée et compétente [06.02.2003].

3.1 Une typologie de la menace

La sécurité de l'information doit faire face à quatre catégories de menaces, classées en fonction du degré de structure de leur organisation et du fait qu'elle soient internes ou externes à l'organisation à laquelle leur cible appartient :[12]

- Les **attaquants externes et non-structurées**, (*hackers* ou *crackers*) n'ont pas beaucoup de moyens à consacrer à leur tâches, n'ont pas d'accès aux systèmes-cibles, et manquent de persistance : si leur cible est trop bien protégée, ils passent à une autre. Ils ont par contre du temps et peuvent agir dans la durée. Bien que figurant souvent au sommaire des magazines, ils ne sont pas forcément les plus dangereux.
- Les **assaillants externes et structurés**. Travaillant pour des organisations étatiques ou non, ils disposent de connaissances étendues, de persistance et de temps.
- Les **agresseurs internes** (structurés ou non). Ils posent une menace sérieuse car ils se trouvent déjà à l'intérieur du système, au delà des lignes classiques de défense. Disposant des connaissance, de persistance et de l'accès, ils posent le défi le plus important à l'organisation dont ils font partie. Les mesures de protection techniques doivent être renforcées par des mesures organisationnelles.

3.2 L'avantage de l'attaque face à la défense

A ceci s'ajoute une dissymétrie entre l'attaque et la défense. L'attaque devient de plus en plus facile puisque des scripts d'attaques peuvent être téléchargés de sites Internet et utilisées par des personnes sans formation particulière.[13] Le site de *Gibson Resarch* www.grc.com a été attaqué et mis pour un temps hors service par un adolescent de treize ans.[14] Les attaques de début février 2000 contre les sites de Google, eBay, Amazon, CNN, ETrade et Excite ont été menés par un *teen-ager* de 15 ans, MaffiaBoy.[15]

La défense est rendue toujours plus difficile par la complexité croissante des systèmes et leur mise en réseau. La sécurité des systèmes informatiques contemporains ne figure pas au premier plan de leurs caractéristiques. D'autre part, la probabilité de trouver toutes les failles d'un système complexe (défense) est de plusieurs ordres de magnitude inférieure à celle de découvrir une seule faille (attaque).[16]

Il faut donc s'attendre, dans les prochaines années, à une intensification de ces attaques et à une aggravation de leurs conséquences.[17]

Finalement, la technologie de l'information permet une dissymétrie entre les attaquants et les attaqués : Il est possible à des individus ou à des groupes sans grand moyens de s'attaquer à des organisations ou à des nations.

---

[12] Basé sur Waltz, Edward*, Information Warfare Principles and Operations*, Artech House, 1989, ISBN 0-89006-511-X, pp 304 – 307. La classification de Waltz est elle-même basée sur Doty, T., *Internet Security : Vulnerabilities, Threats and Mitigation*, ACM Professional Development Seminar, University of Maryland, Nov 1997.

[13] Voir, par exemple Anderson, Ross, *Security Engineering, A Guide to Building Dependable Distributed Systems*, Wiley Computer Publishing, 2001, ISBN 0-471-38922-6, p. 369 sq.

[14] Une description complète de ce cas est disponible sous http://grc.com/dos/drdos.htm [06.05.03].

[15] Barabási Albert-Lázloó*, Linked The new Science of Networks*, Perseus Publishing, 2002, pp 3-5.

[16] Anderson, Ross, *Op. Cit.*, pp. 523-526.

[17] *Ibidem*, pp. 387-388.

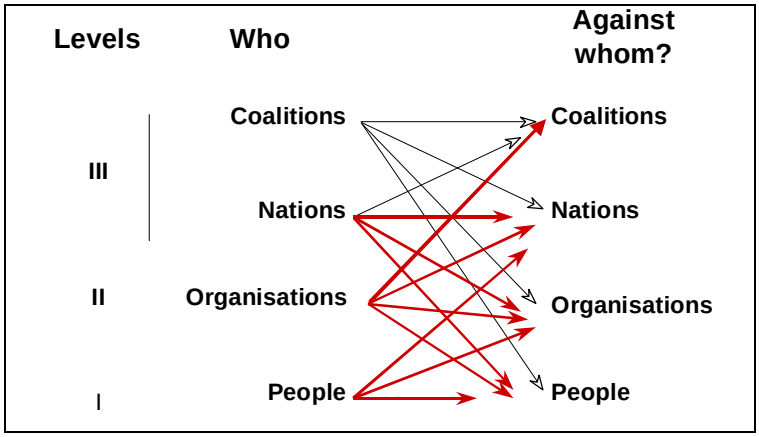

Figure 5 : Dissymétrie entre attaquant et attaque. [18]

3.3 Synthèse : le temps et l'attaque appliqués à la technologie de l'information

On considère généralement que la sécurité de l'information est basée sur trois fonctions principales :[19]

- La **disponibilité** ;
- **L'intégrité** ;
- La **confidentialité**.

Pour attaquer la disponibilité d'un système, on emploie des méthode de déni de service (*Denial of Service*, DoS). Le système est soumis à un flux ininterrompu de messages qui mettent ses capacités de traitement à genoux. Il s'agit clairement d'une utilisation de la dissynchronicité. Un DoS peut être rapidement détecté. Au pire, une solution provisoire peut consister à retirer le système du réseau d'où provient l'attaque.
Pour s'attaquer à l'intégrité ou à la confidentialité d'un système, il faut utiliser l'asynchronicité. C'est ce qui rend la détectabilité de ces agressions difficile. Ce d'autant plus si l'attaque est menée de l'intérieur.

3.4 Justification de la deuxième thèse

L'attaque asynchrone est difficile à détecter car elle peut se fondre dans le bruit. Pour un adversaire qui agit de manière dissymétrique, c'est la manière la plus simple d'arriver à son but. De plus, si les systèmes actuels sont plus ou moins bien protégés de l'extérieur, ils ne le sont généralement pas de l'intérieur. Dès lors, il est clair que la menace a perdu son caractère symétrique et extérieure et qu'elle est interne et / ou dissymétrique.

4 Un but possible : l'infrastructure d'information critique

4.1 La notion de centres de gravité

Le centre de gravité est un point d'application particulier de la force défini initialement par Clausewitz.[20] Nous en proposons la définition suivante, plus adapté au monde contemporain :
« *Les **centres de gravité** sont des points du système ennemi sur lesquels l'emploi de la force opérative va in fine produire des effets recherchés qui amènent l'adversaire à se comporter dans notre sens.* »

---

[18] Schwartau, Winn, in Nicander, Lars D., *Information Operations/Information Assurance – A Swedish View*, Presentation 13 June at INFORMO 2001.

[19] Walz, *op. cit*, p 310 sq.

[20] „*Es kommt darauf an, die vorherrschenden Verhältnisse beider Staaten im Auge zu haben. Aus ihnen wird sich ein gewisser Schwerpunkt, ein Zentrum der Kraft und Bewegung bilden, von welchem das Ganze abhängt, und auf diesen Schwerpunkt des Gegners muss der gesammelte Stoss aller Kräfte gerichtet sein*." Clausewitz, *Vom Kriege*, Auswahl, Philipp Reclam Jun : Stuttgart, Bibliographischergänzte Ausgabe, 1995, p. 315.

Dans la littérature militaire moderne, les centres de gravité sont modélisés sur le concept des cinq cercles du colonel américain John Warden III.[21]

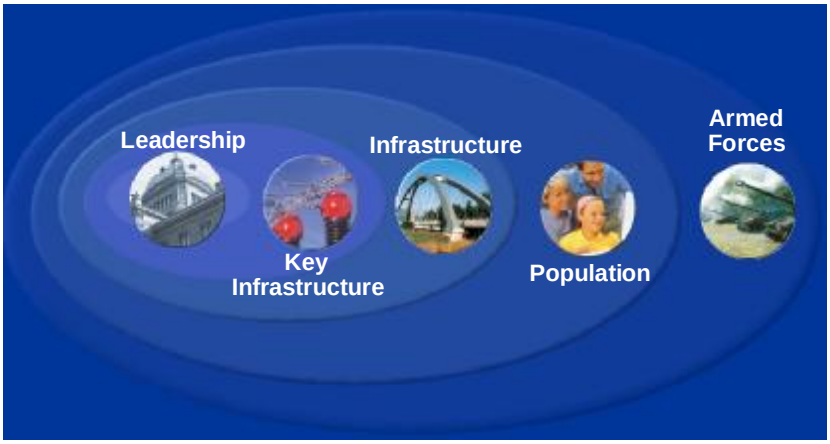

Figure 7 : Centres de gravité ; les cinq cercles de Warden.

Pour Warden, le cercle le plus important est celui du **commandement**. S'il est éliminé ou ne peut plus conduire, la direction des opérations est rendue très difficile.
Le deuxième cercle critique suivant est celui de **l'infrastructure clé**. «*Il s'agit des installations et des processus sans lesquels l'Etat et son organisation ne peuvent se maintenir*»,[22] comme les installations de production énergétique.
Le troisième cercle celui de **l'infrastructure**, comme les moyens de transport, les routes, etc. Ces installations sont plus nombreuses que celles de l'infrastructure clé. Leur redondance les rend difficile à mettre hors d'état.
Le quatrième cercle est celui de la **population**. L'attaquer directement n'est pas compatible avec l'éthique contemporaine et les bombardements sur l'Allemagne et la Grande-Bretagne pendant la Seconde Guerre mondiale ont démontré la force de résistance des sociétés. Une approche indirecte semble plus utile.
Le cinquième cercle est celui des **forces armées**. Si leur destruction peut mettre fin à une guerre, il est plus économique de s'attaquer en premier lieu à leur commandement plutôt que de rechercher à anéantir des troupes ou des moyens militaires.

4.2 L'infrastructure d'information critique comme capital stratégique

L'infrastructure d'information critique est définie par le professeur Wenger comme « […] *vernetzendes Führungselement Grundlage für das robuste Funktionieren aller anderen Infrastrukturen [das] ein zentrales Rückgrat unserer hochtechnisierten Gesellschaften [bildet]*».[23] La figure 8 est une représentation hiérarchique possible des classes de systèmes qui forment l'infrastructure d'information critique.

On constate alors que, par le fait que la population, les infrastructures, le gouvernement et les forces armées sont reliées par et dépendent de l'infrastructure d'information critique, celle-ci devient un centre de gravité stratégique dont la mise hors service, même partielle, permet d'influencer de manière indirecte la décision politique. Les forces armées et le

---

[21] Voir Warden III, John A*., L'ennemi en tant que système*, Texte publié dans *l'Air Power Journal*, printemps 1995, et traduit par le Comité de réflexion et d'études stratégiques aérospatiales de l'Association des anciens élèves de l'Ecole de l'Air, Internet : http://www.stratisc.org/strat/strat_059_Warden.html [05.02.03] et l'ouvrage séminal du même auteur, *The Air Campaign: Revised Ed*., ToExcel, Reprint edition, 1998, ISBN: 1583481001.

[22] Warden, *L'ennemi en tant que système*.

[23] Wenger, Andreas, *Critical Information Infrastructure Protection: Der Staat als Anbieter von Sicherheit im Informationszeitalter,* Vortragsreihe Informationstechnik und Armee (ITA) an der ETH Zürich, 23.10.02, Cf. *supra*.

gouvernement peuvent disposer des réseaux les mieux protégés, ils n'en demeurent pas moins -indirectement- vulnérables.
Il ne faudrait cependant pas en conclure l'inanité de protéger et de séparer les réseaux de conduites stratégiques de l'infrastructure civile, dans la mesure où ils pourraient, en cas d'attaque conséquente, permettre la conduite subsidiaire de la phase de réaction jusqu'au retour à la situation antérieure.[24]

4.3 Justification de la troisième thèse

En raison de sa place centrale dans les pays développés, l'infrastructure d'information critique représente un centre de gravité stratégique.

5 La solution : holistique et intelligente

La détection d'attaques asynchrones et asymétriques ainsi que la problématique de l'attaque interne revêtent dimension stratégique lorsque l'on prend en considération l'infrastructure d'information critique.
Les servitudes relatives à la protection de l'infrastructure d'information peuvent être résumés comme suit :

- Une capacité de réaction vingt-quatre heures sur vingt-quatre est indispensable, ne serait-ce qu'en raison du caractère global de la menace
- Le nombre d'attaques va augmenter dans le futur, d'une part en raison du développement des réseaux, d'autre part en raison de la facilité d'utilisation des outils d'attaque
- Il existe une tension entre attaque et fausses alarmes. Anderson relève que l'Internet est particulièrement bruyant : "*a large amount of random crud arrives at any substantial site, and enough of it can be interpreted as hostile to generate a significant false alarm rate*".[25] Il note aussi que, en raison du faible nombre d'attaques qu'il estime à 0.01%o, le rapport entre le nombre de fausses alarmes relativement aux alarmes avérées sera tel que les gardes risquent assurément de manquer les vraies alarmes.[26] Enfin, il observe que les outils de détection d'intrusion de l'US Air Force n'ont jamais détecté d'attaques, alors que d'autres méthodes les ont mises en évidence.

On peut dès lors s'attendre à ce que des attaques aient lieu sous le couvert de fausses alarmes.[27]

5.1 La solution classique

La solution classique aux problèmes de sécurité informatique réside dans l'utilisation des instruments et processus suivants :

- Antivirus ;
- Mise à jour, patching des systèmes d'exploitations et des applications ;
- Détection d'intrusion (Intrusion Detection System, IDS).

Les limites de cette méthodologie sont clairement visibles à chaque attaque importante contre l'Internet :

- La protection de systèmes complexes et de haute valeur nécessite une réel effort, tant dans l'information (Accès et lecture des pages Web des Hackers, lecture des listes de distribution, test de logiciels de hackers, patch) que dans la mise en œuvre

---

[24] Dans ce contexte, voir, par exemple, Anderson, Robert H., *Securing the U.S. Defense Information Infrastructure: A Proposed Approach*, Rand Corporation, 1999, ISBN: 0833027131.
[25] Anderson, Ross *op. cit.*, p 387.
[26] *Ibidem*.
[27] *Ibidem*, p. 388.

- Le patching de systèmes en ligne doit être prudemment testé car le patch peut ne pas être compatible avec certaines applications
- La capacité de réaction à des attaques ou à de fausses manipulations est lacunaire
- L'exemple récent du virus SQL Slammer montre que beaucoup de gestionnaires de systèmes n'appliquent même pas ces mesures de base.

5.2 La solution avancée

Une solution plus adaptée consiste à disposer d'une infrastructure permanente de surveillance (*monitoring*). Cette manière de faire, en parallèle avec une mise à jour suivie des systèmes et des outils de protection, assure un bon niveau de protection. Le facteur temps de réaction lors d'attaques de type DoS est réduit. Par la centralisation, on assure une réponse rapide et à large échelle. Une entreprise peut ainsi se mettre plus rapidement à l'abri d'une attaque.

5.3 Une solution innovatrice

Si la solution du *monitoring* permet une réaction rapide, la détection d'attaque asynchrone demeure malgré tout un probléme. Au delà d'une protection supplémentaire par l'utilisation de lignes de conduites (*policies*), il s'agit avant tout de gagner le temps nécessaire pour prendre les mesures de protection essentielles (Figure 15).
De manière générale, un système de *monitoring* doit obéir aux servitudes suivantes :

- Fonctionnement en parallèle et en collaboration avec les systèmes conventionnels de détection d'intrusion
- Filtre intelligent des alarmes pour limiter le taux de fausses alarmes
- Découvrir les déviations de la normale.

Les systèmes basés sur l'intelligence artificielle (*Artificial Intelligence*, AI) sont adaptés pour réaliser un filtrage intelligent sur la base d'un *data mining* qui, par une extraction de caractéristiques, permet de déterminer quand un comportement du réseau s'écarte de la normale.

5.4 Variante de détection

Le problème principal de détection des comportements anormaux lors d'attaques asymétriques est le fait que les fichiers d'enregistrement (*logging*) ne peuvent être conservés sur de longues durées : La capacité d'enregistrement est limitée. Il faut donc trouver des moyens d'effectuer du *data mining* dans ce fichiers sur une longue période pour déterminer des comportements singuliers. Ces moyens doivent être capables d'apprendre et de s'adapter. Les techniques de l'intelligence artificielle sont particulièrement adaptées à ces tâches. La théorie des réseaux de Bayes[28] trouve ici une application pratique. Ces réseaux sont rapides et ne nécessitent pas de ressources exorbitantes pour leur implémentation. Leur principe probabiliste est particulièrement efficace.

---

[28] "*Bayesian networks get their name from the Rev. Thomas Bayes, who wrote an essay, posthumously published in 1763, that offered a mathematical formula for calculating probabilities among several variables that are causally related but for which (…) the relationships can't easily be derived by experimentation. (…) Bayesian networks are complex diagrams that organize the body of knowledge in any given area by mapping out cause-and-effect relationships among key variables and encoding them with numbers that represent the extent to which one variable is likely to affect another. Programmed into computers, these systems can automatically generate optimal predictions or decisions even when key pieces of information are missing.*" Los Angeles Times, October 28, 1996 cité in Internet : http://www.cs.berkeley.edu/~murphyk/Bayes/la.times.html [09.02.03]. Pour une description plus complète, voir par exemple Murphy, Kevin, *A Brief Introduction to Graphical Models and Bayesian Networks*, last updated October 2001, Internet : http://www.cs.berkeley.edu/~murphyk/Bayes/bayes.html [09.03.02].

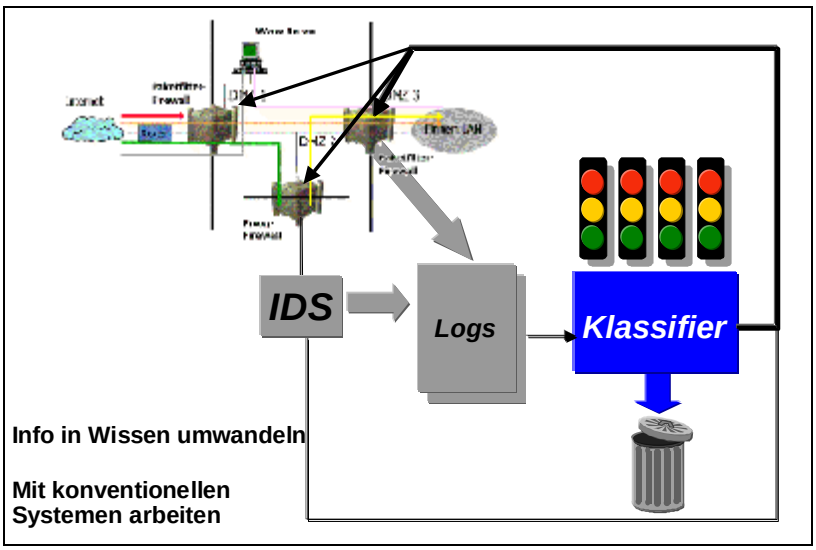

Figure 8 : Réduction des fausses alarmes par classification.

Les données issues des *log files* en provenance du détecteur d'intrusion et du *firewall* (*raw data*), sont traitées par un réseau de Bayes qui en retire les signes distinctifs (*features extraction*). Un autre réseau de Bayes (*classifier*) classifie les signes distinctifs et en retire des indication de normalité. Sur cette base, un traitement ultérieur (*post processing*) basé sur des règles déterminées déclenche l'alarme en fonction des indications de normalité.

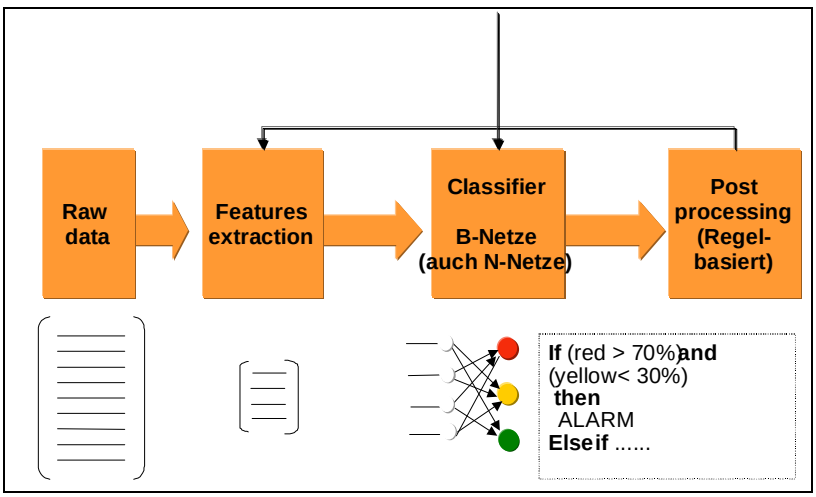

Figure 9 : Structure du classificateur.

L'apprentissage de la normalité est réalisé en faisant traiter par le réseau des données issues de configurations sans attaques. Le traitement de *log files* issus de systèmes attaqués permet de différencier entre bruit et attaque. Le fait que le réseau soit capable d'apprendre rend transparentes les modifications du système comme, par exemple, l'addition de nouveaux ordinateurs dans le réseau ou de nouvelles connexion.

5.5 Variante de correction

La variante présentée ci-dessus permet de détecter des attaques externes plus rapidement que des systèmes conventionnels. Par contre, il ne supporte pas les administrateurs dans leur tâche de réaction, pas plus qu'il ne sert à défendre un réseau

contre des attaques internes. La variante proposée ci-dessous permet de décentraliser la protection. Elle applique la conception biologique des globules blancs à un réseau. Le *firewall* et le détecteur d'intrusion sont répartis dans le réseau. Les « globules blancs » électroniques circulent dans le réseau sous une forme semblable aux virus, indépendants du système d'exploitation.
Dans l'implémentation proposée, trois types de globules blancs sont implémentés : des **détecteurs**, qui « patrouillent » dans le réseau et repèrent toute anormalité. Dans ce cas, ils marquent l'élément suspect et émettent un équivalent virtuel de phéromone qui attirera les censeurs. Les **censeurs** évaluent si l'élément douteux appartient au système ou non. Si oui, ils bloquent l'émission de phéromone et se détruisent. Dans l'autre cas, ils émettent davantage de phéromone et attirent les « **cellules tueuses** ». Elles détruisent les éléments marqués et la phéromone. Le cas échéant, elles sont capables de couper la partie du réseau infectée du reste. L'approche biologique permet une implémentation très simple : en temps normal, elle ne requiert qu'environ 5% de ressources.

5.6 Conséquence

L'approche présentée ici est simple et assiste les administrateurs de systèmes : le concept aide à gagner du temps et à réagir rapidement en cas d'attaque contre un réseau. La détection de l'anormalité permet également de prendre influence à l'intérieur d'un réseau et d'avertir les responsables en cas de fausse manipulation ou de négligence.
Ce système, en cours de développement, n'est naturellement pas la panacée et il n'est applicable qu'en parallèle avec des solutions classiques, comme des détecteurs d'intrusion, des *firewalls* et la définition de lignes de conduites (*policies*) cohérentes.
Les réseaux de l'infrastructure informatique critique sont de nature hétérogène. La rapidité de réaction et la large palette des risques auxquels ils sont confrontés en font des candidats optimaux pour l'application de ces techniques novatrices.

5.7 Justification de la quatrième thèse

Face à une potentialité de menaces asymétriques et asynchrone contre les réseaux informatiques, plus particulièrement contre l'infrastructure d'information critique, les solutions classiques ne suffisent plus. Elles doivent donc être complétées par des systèmes innovateurs.

6 Conclusions

Cet exposé aura montré les points suivants :

- La maîtrise du facteur temps est la condition préalable du succès. La surprise est atteinte par la symétrie ou la dissymétrie.
- La menace a perdu son caractère symétrique et extérieure. Elle est interne et / ou dissymétrique.
- L'infrastructure d'information critique représente un centre de gravité stratégique.
- Au vu de ce qui précède, les solutions de protection classiques doivent être complétées par des systèmes innovateurs.

7 Choix de questions posées à l'issue de la conférence

Question : Plutôt que d'augmenter la complexité du système par des « globules blancs », ne devrait-on pas augmenter la formation et le nombre des administrateurs de réseau ?

- Réponse : La complexité dans un réseau est causée par les connections entre les éléments du système. En temps normal, les « globules blancs » travaillent de manière indépendante et ne procèdent pas de la complexité globale. Quand à la formation des

administrateurs, elle ne permet pas in fine d'augmenter la rapidité de réaction face à une attaque. L'augmentation du nombre est limitée par les frais de personnel et la disponibilité du marché.

Question : Dans la réflexion sécuritaire classique, on relève l'avantage à la défense. Est-ce encore le cas ?

- Réponse : Nous avons relevé la problématique de la dissymétrie entre la défense et l'attaque dans le domaine de la technologie de l'information. Le fait que l'attaque soit toujours plus facile et ne demande plus de connaissance ou de compétence technique rend la défense, dont la complexité augmente continuellement, beaucoup plus difficile. La solution proposée permet dans une certaine mesure de combler ce fossé.

Question : La doctrine chinoise de l'«* Unlimited Warfare *» est-elle vraiment représentative de la stratégie chinoise ?

- Réponse : L'appréciation de la validité de cette assertion du point de vue de la sinologie dépasse nos compétences. Le point important est le suivant : Un pays ou une organisation qui souhaite se confronter aux Etats-Unis ou à l'OTAN ne va pas utiliser de stratégie symétrique. La défaite de l'Iraq en 1991 a servi de leçon. Une conception indirecte ou asymétrique est par contre susceptible de succès. L'infrastructure d'information critique apparaît comme une cible possible pour ces attaques.

8 Remerciements

L'auteur remercie Monsieur Stefan Burschka, Swisscom Fixnet SA, pour son assistance substantielle à la préparation de cette conférence.