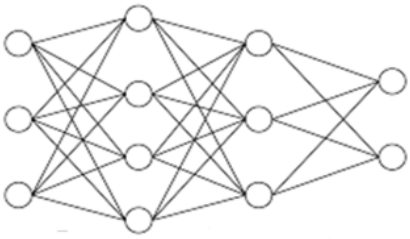
Le rapport de force dynamique

Djamel Metmati

Chaire de cyberdéfense & cybersécurité Saint-Cyr, Sogeti, Thales

Mars 2017 – Article V. 6

Résumé : Avec l'emploi d'Internet dans le domaine de la guerre, l'introduction de la dimension cyber en accompagnement de l'action militaire démontre qu'une organisation est capable d'établir une stratégie et une tactique en employant des techniques spécifiques émanant du rapport de force dynamique.
Un rapport de force consiste à établir une relation de puissance entre des parties ennemies, alliées ou neutres où se confrontent des forces contraires à des moments et à des lieux précis. Or, son caractère dynamique traite de l'utilisation de la non-linéarité des communications depuis l'introduction du numérique dans les transmissions (voir schéma 1). Ainsi, le rapport de force dynamique consiste en l'étude d'un système militaire ou civil en le partitionnant en un nombre fini de régions et en s'intéressant aux trajets possibles des données dans ces régions lorsque le système est contraint de s'auto-adapter aux conditions de transmissions et aux menaces sur les données jusqu'à leur destination.
Si ces différentes technologies aident à la résilience des réseaux, elles donnent également naissance à l'intelligence numérique. Cette méthode produit des typologies d'attaques et de défense fines rendues possibles par l'exploitation du rapport de force dynamique propre à la mobilité des réseaux.



Emission ➞ Interconnexions invisibles ➞ Réception
Schéma 1

I- Comprendre le rapport de force dynamique

Le rapport de force dynamique pourrait se définir comme une relation entre les forces et les dynamiques que produit tout échange de données dans les réseaux. Il créé de l'intelligence numérique qui se traduit par la capacité à se représenter des informations ou des grandeurs physiques et de pouvoir mettre en œuvre des procédés ou des actions offensives ou défensives à mon avantage. Des dispositifs d'exploitation permettent la visualisation et l'interprétation de ces informations parfois complexes et, de cette manière, peuvent concourir à la réalisation d'un rapport de force au profit de l'action civile et militaire.

Gérer la complexité est la norme dans la conduite d'une opération militaire car celle-ci intègre des interconnexions entre systèmes et un accroissement notable des données à traiter. Depuis les années 90 jusqu'à l'intervention militaire contre Daesh, l'interconnexion des systèmes nationaux avec les systèmes des coalitions internationales génère des échanges pour planifier et conduire des manœuvres conjointes. Désormais, le raisonnement militaire intègre cette complexité dans toutes les phases d'une opération, ce qui prend la forme d'une intelligence dite numérique. La méthode opérationnelle consiste à employer des réseaux fixes et mobiles pour conduire des feux et des appuis et coordonner l'action des engins autonomes. Ainsi, les drones tactiques et stratégiques permettent de mener des actions à distance étant des vecteurs aériens autonomes dépendant des réseaux et de leur système d'exploitation embarqué et temps réel. Autre exemple, la gestion des unités passe par la collecte d'informations via les systèmes de transmission et leur restitution sur des interfaces graphiques. Dès lors, le manque d'uniformité de ces systèmes crée des suites possibles de posture d'attaque ou de défense à partir de ces faiblesses potentielles que sont les nœuds de communications[1]. La tactique numérique peut s'appuyer sur les vulnérabilités de ces interconnexions qui pour la plupart ont des configurations techniques différentes. L'écoute du trafic par des sondes permet de comprendre les mécanismes d'aiguillage des données. Ce sont les marqueurs qui permettent le suivi de l'information, qu'elle transite via une onde radio ou qu'elle emprunte un autre réseau via des passerelles identifiées. Le mécanisme de propagation des données s'appuie sur la théorie des systèmes dynamiques[2] appliquée aux fonctionnements automatiques des transmissions entre un point d'émission et de réception.

Or, une opération militaire implique une adaptation constante de ses systèmes de transmission au niveau des postes de commandement et des unités. La construction d'une stratégie et d'une tactique de combat numérique nécessite la prise en compte des risques liés à ces changements et aux vulnérabilités qui en découlent.

Les cibles et les effets de la cyber-campagne russe contre la Géorgie en 2008[3] ont montré un emploi possible du rapport de force dynamique en appui d'une opération militaire. Malgré la

---

1 Une faible densité d'interconnexions des réseaux se définit par du soft « network ». En revanche, une forte densité d'interconnexions peut être qualifiée par « hard network ».

2 La théorie des systèmes dynamiques se développe à la frontière de la topologie, de l'analyse, de la géométrie, de la théorie de la mesure et des probabilités. Ce concept a été introduit par Poincaré à la fin du XIXème siècle.

3 Special Report august 2009 overview by the US-CCU of the cyber campaign against Georgia.

mise en place de filtres sur les sites institutionnels géorgiens et la délocalisation de leurs serveurs sur d'autres territoires, les attaquants ont réorienté le trajet des données par une attribution d'identifiants différents. Les interférences provoquées ont modifié le processus des paiements et des transactions financières de la banque nationale géorgienne. Pour autant, si le but de notre exposé est de comprendre l'évolution à long terme d'un système, son interprétation dépend qualitativement et statistiquement du cas étudié et des outils de mesure utilisés[4]. Comme le définit la mécanique quantique[5], la compréhension d'un phénomène dépend de l'outil de mesure et du moment où l'observation est constatée : deux mesures identiques peuvent avoir des résultats différents au regard de ces deux conditions. Plus la dynamique des échanges est élevée, plus l'entropie du système est élevée, ce qui se traduit par une imprédictibilité à long terme de l'état du système en dépit de sa connaissance et de sa maîtrise initiale du fait d'une architecture de communication supposée figée.
Même s'il existe des solutions pour la détection d'attaques, les outils ne sont jamais totalement adaptés aux effets du comportement humain. Un système d'arme interconnecté à d'autres systèmes adopte un comportement déterministe si sa programmation répond à des instructions préétablies (méthodes formelles). Ainsi, les systèmes de contrôle automatisés et les systèmes d'armes sont vulnérables à des cyber-attaques dès lors que sont connus leurs comportements déterministes et qu'il devient possible d'anticiper leurs états. Un système auto-apprenant pourrait ainsi s'adapter à des menaces lorsqu'il constate que ses états sont connus et visités en changeant son comportement.

II- Applications du rapport de force dynamique

Comme il se caractérise par ses échanges d'informations en interne, le système cible se pose en phase initiale comme une citadelle tout en offrant à l'attaquant la possibilité d'une intelligence numérique pour le cibler selon la cyber tactique choisie. Cette méthode emploie des cycles d'action très courts, que permet l'exploitation du rapport de force dynamique. Elle s'applique tant aux cyber-attaques des réseaux civils qu'aux attaques des réseaux militaires stratégiques et tactiques.
Les cyber-opérations russes menées contre les installations électriques ukrainiennes[6] montrent qu'il est possible d'obtenir, par l'attaque de réseaux[7], des effets similaires à ceux obtenus par l'emploi d'armes conventionnelles. C'est en exploitant des vulnérabilités logicielles que les attaquants ont pris le contrôle de l'interface machine gérant l'électricité de sites ukrainiens en

4 Ce que décrit Philippe Baumard sur l'apprentissage continuel de la congruité et incongruité comportementale des interactions machine à machine.
5 Théorème d'incomplétude de Gödel ou les limites de la preuve.
6 Malicious code analysis on Ukraine's power grid incident, Beijing Knowsec Information Technology Co Ltd, V4: 2016/01/10.
7 Black Energy.

2016. Le choix tactique fut de détruire les disques durs des ordinateurs par une infection préalable[8] paralysant l'ensemble du système.
Le niveau de confiance accordé aux systèmes de transmission pour rendre compte de la situation tactique est, aujourd'hui, supérieur à ce qui était fait par le passé. L'introduction de senseurs et de capteurs dans le fonctionnement et la gestion des réseaux de coordination des unités renforcent ce niveau de confiance. La perception et la gestion d'un combat se transforment au rythme de la dynamique de ces systèmes. Ces deux caractéristiques génèrent une nouvelle problématique : la sécurisation des données dans un environnement nouveau et l'instabilité du réseau produit.
On pense notamment à la batterie anti-missile Patriot[9], déployée depuis la première guerre du Golfe, qui a montré que son système de gestion interne pouvait produire des suites d'erreurs[10], qui, cumulés, provoquent une erreur de trajectoire après le tir du missile.
Qui plus est, une cyber-attaque est possible sur l'interopérabilité entre le senseur qui traduit en temps réel les informations entre le lanceur et le système de contrôle, ainsi que la puce qui contrôle le guidage du missile. Tout échange protocolaire, dans un espace et dans un temps défini, constitue, de facto, une source de vulnérabilités. C'est pourquoi, le rapport de force dynamique comprend deux propriétés intrinsèques: les propriétés topologiques du réseau et les propriétés d'acheminement des données.
En y intégrant le déploiement et l'état des liens disponibles, le rapport de force dynamique produit de l'intelligence numérique qui pourrait être mis en oeuvre dans les réseaux civils et militaires.
Par ailleurs se pose la question de la maîtrise des opérations numériques dans lesquelles aucune anomalie n'est détectée alors qu'une modification malveillante du système initial a été réalisée. Par exemple, la prise de contrôle du drone RQ 170 Sentinel par les iraniens en 2011. Grâce à l'emploi de faux signaux GPS, le drone s'est comporté en conformité avec les données reçues alors que son cap et sa destination avaient été modifiés par l'altération des données.

Il est donc nécessaire d'imaginer l'utilisation du rapport de force dynamique sur les bases d'une intelligence capable d'exploiter les identifiants et les protocoles régissant les échanges de données à des fins de détections ou d'attaques.
Il en découle un nouveau champ d'action ou de réaction dû à l'hétérogénéité obligatoire des réseaux déployés.
Ce constat oblige à une bonne maîtrise des mécanismes d'échange d'information au sein de ces réseaux pour anticiper les intrusions et les altérations de données.

8 Le principe des Advanced Persistants Threats. Par exemple, pour n routeurs, n*(n-1)/2 relations adjacentes sont présentes et offrent des opportunités de diffusion de l'attaque.
9 Le cas s'est présenté pour les missiles déployés en Turquie en 2015.
10 Une communication téléphonique produit en moyenne 8 bits erronés par seconde. Et les technologies Ethernet sont basées sur des échanges probabilistes. Ce qui signifie que les réseaux de communications sont imparfaits.