C. Libicki, Cyberdeterrence and cyberwar, Rand corporation | A

Table www.cooperation-iws.eu

1 Martin C. Libicki, Cyberdeterrence and cyberwar, Rand corporation

by admin | décembre 23, 2010 12:48

Rand_cyberdeterence.pdf [1]

<Abstract>

The research described in this report was sponsored by the United States Air Force under Contract FA7014-06-C-0001. Further information may be obtained from the Strategic Planning Division, Directorate of Plans, Hq USAF.

</Abstract>

<Sommaire>

</Sommaire>

<Auteur>

Martin C. Libicki

</Auteur>

Endnotes

1. Rand_cyberdeterence.pdf: /files/papers/cyber-security/Rand_cyberdeterence.pdf

---

11 Comments

admin dit :
2 juillet 2011 à 8:36

1.1 Preface

The basic message is simple: Cyberspace is its own medium with its own rules. Cyberattacks, for instance, are enabled not through the generation of force but by the exploitation of the enemy's vulnerabilities. Permanent effects are hard to produce. The medium is fraught with ambiguities about who attacked and why, about wht they achieved and wether they can do so again. Something that works today may not work tomorrow (indeed, precisely because it did work today). Thus, deterrence and warfighting tenets established in other media do not necessarily translate reliably into cyberspace. Such tenets must be rethought. This monograph is an attempt to start this rethinking.

admin dit :
2 juillet 2011 à 13:59

1.2 Summary

The establisment of the 24th Air Force and US Cyber Command marks the ascent of cyberspace as a military domain. As such, it joins the historic domains of land,sea,air and space.

Cyberattacks are possible only because systems have flaws

Yet system vulnerabilities do not result from immutable physical laws. They occur because of a gap between theory and practice.
(…) There is, in the end, no forced entry in cyberspace. Whoever gets in enters through pathway produced by the system itself. It is only a modest exaggeration to say that organizations are vulnerable to cyberattack only to the extent they want to be. In no other domain of warfare can such a statement be made.

Operational Cyberwar has an important niche role, but only that

For operational cyberwar – acting against military targets during a war – to work, its targets have to be accessible and have vulnerabilities. these vulnerabilities have to be exploited in ways the attacker finds useful.

Strategic cyberwar is unlikely to be decisive

No one knows how destructive any one strategic cyberwar attack would be. Estimates of the damage from today's cyberattacks within the United States range from hundreds of billions of dollars to just a few billion

dollars per year.

(…)
But can strategic cyberwar induce political compliance the way, say, strategic airpower would ? Airpower tends to succed when societies are convinced that matters will only get worse.

Those who would attempt strategic cyberwar also have to worry about escalation to violence, even strategic violence. War termination is also not trivial: With attribution so difficult and with capable third parties abounding (see below), will it be clear when one side has stopped attacking another ?

Cyberdeterrence may not work as well as nuclear deterrence
The ambiguities of cyberdeterrence contrast starkly with the clarities of nuclear deterrence. In the Cold War nuclear realm, attribution of attack was not a problem; the prospect of battle damage was clear; the 1000th bomb could be as powerful as the first; counterforce was possible ; there were no third parties to worry about; private firms were not expected to defend themselves; any hostile nuclear use crossed an acknowledged threshold; no higher levels of war existed; and both sides always had a lot to lose. Although the threat of reteliation may dissuade cyberattackers, the difficulties and risks suggest the peril of making threats to respond, at least in kind. Indeed, an explicit deterrence posture that encounters a cyberattack with obvious effect but nonobvious source creates a painful dilemma: respond and maybe get it wrong, or refrain and see other deterrence postures lose credibility.

Will we know who did it ? Cyberattacks can be launched from literally anywhere, including cybercafés, open Wi Fi nodes, and suborned third-party computers.

> On remarque la rhétorique bien réglée de la dissuasion nucléaire, qui précise qu'on sait obligatoirement qui est responsable. On s'aperçoit donc ici comment les américains forgent les croyances sur la dissuasion nucléaire, chez leurs alliés mais également chez leurs ennemis. Ce mécanisme, c'est d'ailleurs spécifié dans le texte, repose sur la réputation. Or nous savons bien aujourd'hui, qu'il est possible d'utiliser l'arme nucléaire sans forcément, signer l'acte comme pourrait l'illustrer l'utilisation des effets d'une explosion sous-marine sur une faille tectonique.

admin dit :
3 juillet 2011 à 12:51

1.3 Chapter one Introduction

Finally, while we hope this work has international applicability, it was written from the US perspective, in particular, the perspective of a country that has invested so much in processes that depend on cyberspace.

> On remarque en effet les milliards de dollars investis dans Internet aux cours des années, ainsi que le fait qu'aujourd'hui, l'économie américaine repose en grande partie sur les ténors, les multinationales du numérique. Ces multinationales numériques n'ont d'ailleurs pas d'équivalent dans d'autres pays du monde, pour des raisons que nous définirons par la suite.

admin dit :
5 juillet 2011 à 14:58

1.4 Chapter two A conceptual framework

Cyberspace is a virtual medium, one far less tangible than ground, water, air, or even space and the RF spectrum. One way to understand cyberspace in general, and cyberattacks in particular, is to view it as consisting of three layers: the physical layer, a syntactic layer sitting above the physical, and a semantic layer sitting on top.

Internal threats
States have two other methods of gaining access to systems; in fact these are the only ways to get into truly closed systems.One is to recruit insiders, who, with varying degrees of help, can introduce mischief into systems. The other is to toy with the supply chain so that target systems contain components that appear benign but contain code that respond to a state's directions or at least priorities.

Insiders
Unlike operating a system connected to the rest of the world, which is known to contain hackers, operating one from the inside to create mischief tends to violate explicit trust conditions.
(…)
The insider threat has always been a staple of computer security, not least in the banking industry.

Supply Chain
Notable cases of successfully compromised components include (1) the British donation of Enigma machines to other nations, which likely did not realize that the British were able to break and thereby read messages from such machines and (2) the installation in the soviet natural gas network of (black market) systems controllers altered to malfunction in ways that lead to destructive pipeline explosions. There are also suspicions that some cryptographic devices a Swiss company sold had a National Security Agency (NSA) - sponsored back door. Many in the defense community worry that China's growing presence in component manufacturing provides it plenty of opportunities for mischief - which it may not be shy about taking advantage of.

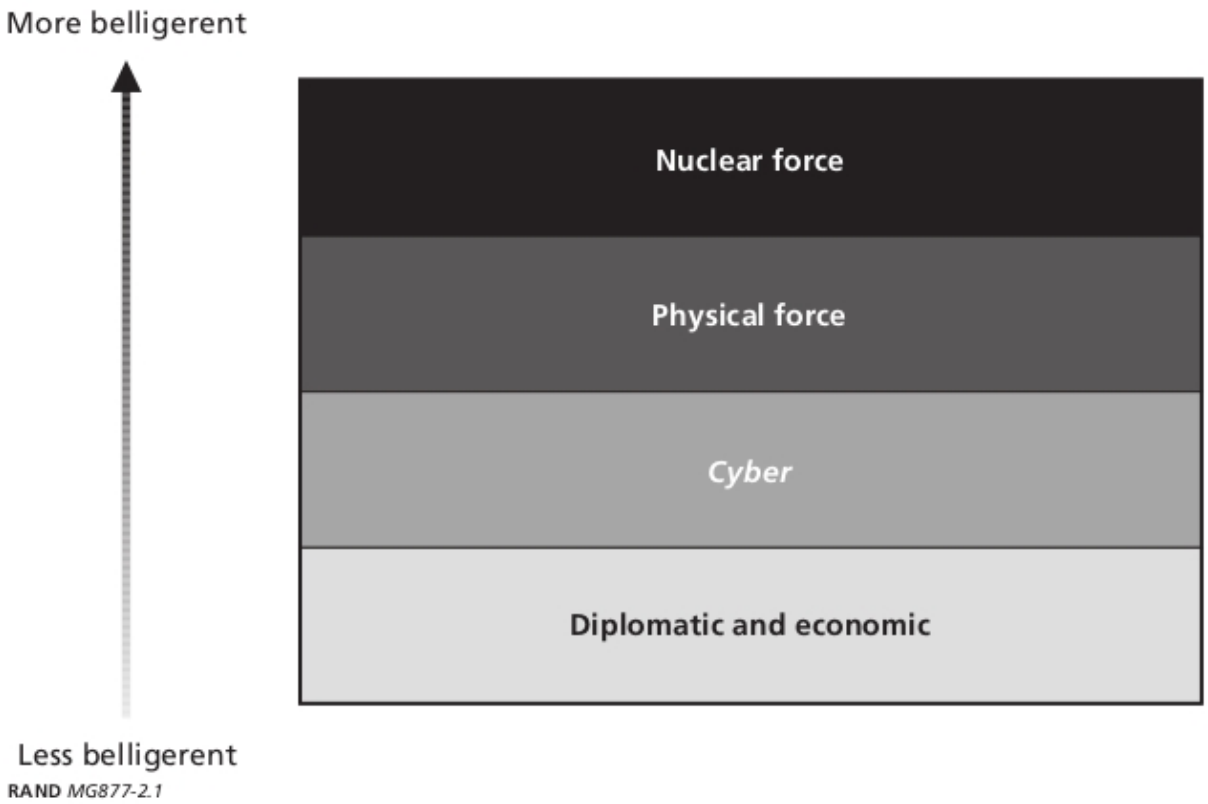
Unless and until purchasers get access to all the code in the electronics they buy, a supply chain attack is difficult to defend against.

-
On remarque ici la mention de « supply chain attack », d'attaque de Chaines d'approvisionnement, de chaînes logistiques. Cette mention dans un document publié en 2008, démontre ainsi que le concept de guerre économique existe, qu'il est théorisé et utilisé par les américains, qui manifestement ne s'en cachent pas.
On remarque également, que cette notion d'attaque des chaînes d'approvisionnement est associée à une notion de timidité. Ce propos marque assez bien l'ironie des pays industrialisés européens qui ignorent encore les mesures à prendre pour protéger leurs économies contre ce type d'attaque, comme l'illustre les cas du fabricant de carte à puce GemPlus, du quasi monopole du système d'exploitation Windows sur les systèmes informatisés européens, ou plus récemment des externalisations chez les systèmiers de l'automobile et de l'aéronautique …
La maîtrise de la chaîne d'approvisionnement est une priorité pour sauvegarder l'intégrité des systèmes, des données mais également de l'emploi. C'est une priorité que les Etats Unis d'Amérique placent au niveau fédéral, aux plus hauts niveaux décisionnels du gouvernement.
Une attaque de chaîne d'approvisionnement est typique d'un contexte de guerre hors limite, utilisant la déception pour s'emparer sans violence des forces vives d'un pays considéré comme un ennemi ou un rival, de son économie. On illustrera par l'expression « retirer des bûches sous la marmite » (/Philoblog-2/?p=233)
On remarquera également combien l'idée de maîtrise de la chaîne d'approvisionnement est éloignée de l'externalisation et autres privatisations véhiculées par les gourou du management pendant les premières heures de la mondialisation internet.
-

Defining Cyberattack
With that as background, cyberattack, for the purpose of this discussion, is the deliberate disruption or corruption by one state of a system of interest to another state. The former state will be refered to as the attacker; the latter state will be refered to as the target. In some contexts, the target may also become a retaliator.

Likewise, this definition of cyberdeterrence does not include such lesser measures as prosecuting hackers themselves or taking diplomatic or economic measures, although Chapter Five does touch on lesser measure. This is not to say that the threat of such measures cannot dampen the other side's aggressiveness in cyberspace – they may, in fact, be the better course of wisdom. However, if something less aggressive sufficed, why bother with cyberdeterrence ? Again, expanding the definition is unnecessary for tackling the many issues discussed here. Similarly, for purposes of discussion, this definition does not entail cyberresponses to other types of attacks (although Chapter Four does touch on this) Figure 2.1 depicts four types of response, listed in rough order of level of belligerence (although not necessarily the magnitude of the consequences).

Figure 2.1
Responses by Rough Order of the Level of Belligerence



On remarquera que le schéma ne possède pas de niveau 0. En d'autres termes, il n'existe pas de place pour la paix, pour la coopération, le premier niveau étant celui des relations économiques et des relations diplomatiques. On le rappelle, nous sommes ici en train de parler de niveaux de belligerrence, de niveaux de guerre. Ainsi, célébrées par des auteurs comme Machiavel ou De Callières (.//?p=86), les modalités guerrières d'une relation économique, d'une relation diplomatique sont loin d'être quelque chose de dissimulé, puisque cet aspect figure dans des publications gouvernementales.

Deterrence in general comes in many forms. Some forms are singular, while others have to be repeated. Some are asymmetric and some are symmetric (among peers).
Nuclear deterrence is singular and symmetric. It is singular in the the point is to make the prospect so frightening that no one dares invoke it.

The expenditure of U.S organizations on information security easily measure in the tens of billions of dollars a year – yet security breaches occur daily. This is why the federal government sought $7.3 billion in fiscal year 2009 to protect government computers over and above the billions already spent.

(…) Damage to sensitive information systems could be much greater than even the owners know because a great quantity of rogue code could be hiding, awaiting an activation signal. estimates of over $100 billion worth of annual damage in the United States alone are common.

admin dit :
6 juillet 2011 à 14:40

1.5 Chapter three Why Cyberdeterrence is Different

Cyberdeterrence seems like it would be a good idea. Game theory supports the belief that it might work. The nuclear standoff between the United States and the Soviet Union during the Cold War – which never went hot – provides the historical basis for believing cyberdeterrence should work.

Do we know who did it ?
The notion that the one should know who attacked before retaliating seems clear enough. If deterrence is to work before the first retaliation takes place, others must have confidence that the deterring state will know who attacked it. Hitting the wrong person back not only weakens the logic of deterrence (if innonence does not matter, why be innocent ?).

(…) Even if the effects are public, the cause of the malfunction may be apparent only to the target (if correct) and the attacker (who will likely correlate the failure of the target system with its having been attacked). If retaliation is to be public, deterrence must likewise be public.

(…) Attribution may be so uncertain that the odds that any one cyberattack could evoke a response would be fairly low. How low can the odds of attribution fall without destroying the empirical basis for deterrence ?
The raw calculus of deterrence is fairly straightforward: The lower the odds of getting caught, the higher the penalty required to convince potential attackers that what they might achieve is not worth the cost. Unfortunately, the higher the penalty for any one cyberattack, the greater the odds that the punishment will be viewed as disproportionate – at least by third parties (who will not know what the attacker did get away with) and perhaps even by the attacker. In other domains with low catch rates (e.g., traffic violations, marijuana possession), the accused at least know that they were caught because they were guilty.
What makes attribution so hard ? In a medium where « nobody knows you're a dog », it is equally hard to know wether you are a hacker.

On remarque ici le coeur de la problématique, qui consisterait à identifier tout le monde, à ficher tout le monde.

Finding rogue packets that can be traced back to the network (IP) address of a government bureaucracy reveals a bureaucracy that is stupid, is arrogant, runs so many hackers that it cannot be anything less than obvious, or operates a network that has been hijacked by others. Packet can be bounced through multiple machines on their way to the target. They can be routed through a bot that only needs to erase the packet's originating address and substitute its own to mask the true origin. Attacks can be implanted beforehand in any machine that has been compromised.

(…) For example, evidence that an attack used heavyweight code-breaking would normally point to a state attacker because traditionally, private hackers could not afford the supercomputers necessary for such a task.

> Cet élément explique pourquoi dans le cadre d'une perte de la maîtrise des approvisionnements, les PC, en majeure partie d'origine américaine, vendus dans la distribution grand public ne dépassent pas 4GB de RAM depuis bientôt 4 ans, alors que parallèlement en s'approvisionnant en pièces détachées, des cartes mères d'origine asiatique supportent 8GB de RAM depuis 3 ans, et qu'aujourd'hui 16GB de Ram est considéré comme un minimum. Plusieurs éléments favorisent ce phénomène d'une part des systèmiers électroniques sous influence américaine, d'autre part un système d'exploitation monopolistique d'origine américaine également. Il ne revient pas de trancher en quoi casser un code cryptographique pour un particulier est quelque chose de bien ou de mal, mais plutôt de voir comment une perte de maîtrise de la chaîne d'approvisionnement a une incidence sur la population et exerce une action politique, une action géopolitique.

Can we hold their assets at risk ?

Can we do so repeatedly ?

Deterrence can be fragile if hitting back today prevents hitting back tomorrow and thereafter. For most forms of deterrence, this is not a problem. Some deterrents are so awful that no one temps them. For others, one hit does not preclude another. In cyberspace, the problem is vexing. serial reapplication of retaliation may be necessary, but each use tends to diminish the expected consequences of the next use.

(…)
All this weakens an implied promise of deterrence: If you stop, we stop. With the existence of third-party hackers, the « we » loses its strength. What attackers want to hear – if you stop, it stops – may not be something the retaliator can promise. Fortunately, third-party attackers mays strengthen an implied threat of deterrence: Do not even start because who knows where it will lead.

> On remarque qu'en quelque sorte, le document fait les questions et les réponses à la manière d'une description d'un jeu en théorie des jeux (voir Schelling, the Strategy of conflict .//?p=38), à la manière dont on forge une névrose ou une croyance également. On rapprochera

ce commentaire de celui ci .//?p=143#comment-263

Does retaliation send the right message to our own side ?
Some potential cybertargets are government systems and some are private. The latter set includes almost all U.S energy, communications, and financial infrastructure. Severe attacks on them are likely to get the public's attention. With a few exception (discussed later), government systems are not so essential to day-to-day life. The defense of private systems is largely in private hands. Although the goverment can play a key indirect role in protecting such systems (e.g through the development of policies, standards, and law enforcement), it can do little directly. the goverment has no privileged insight into specific vulnerabilities of private systems, and there is little evidence that private system owner are interested in telling it.

> On remarque la dichotomie public, privé révélatrice de la méthode de gestion anglo-saxonne. On s'interroge sur ce point, car de nombreux éléments tendent à montrer que cette dichotomie public, privé est un leurre exploité à des fins de déceptions par les américains. En effet, on remarquera l'obéissance systématique et servile des moyens de communications, des médias anglo saxons et des pays sous influence, à la communication commerciale de ces grands firmes privées ; obéissance qui ne peut se faire qu'avec une aide gouvernementale, un appui cohercitif militaire. On remarquera aussi que la baronie qui siège dans les conseils d'administration de ces firmes privées exercent un contre -pouvoir aux volontés gouvernementales, par l'instauration de cette dichotomie public, privé dans les domaines qui concernent cependant et largement tous les aspects de la vie et de la subsistance des populations.

Ironically, a government deterrence policy may weaken rather than strengthen the private sector's incentive to protect its own systems if that policy alters who is responsible for third-party damage. If the power industry, for instance, fails to protect its supervisory control and data acquisition system, and then gets hacked into and shut down, the cost to its users (i.e., blackouts) far outweighs the lost revenue to the power company. The threat that angry customers could sue the company and recover damages (or that regulators will get angry) has to be uppermost in the minds of the power company's security managers. The same holds in general for public or at least publicly accessible infrastructures.

> On remarque le raisonnement alambiqué clamant que la régulation gouvernementale se fait au détriment du consommateur. Ce dernier, se voyant en effet, privé de recours juridique face à l'Etat. Ce passage illustre assez bien comment le système judiciaire américain est utile à la vie démocratique et pourquoi la classe ou la caste juridique se forme au détriment du reste de la population.

Do we have a threshold for response ?
Strict adherence to a no-threshold policy of response also implies a no-threshold policy of investigation of cyberattacks, one that is untenable and, in any case, unaffordable.

If adversary believes that it can carefully calibrate increasing levels of attack – extremely hard to do in practice – it may hope to replicate what happens to frogs put in slowly boiling water: No gradient pain is sharp enough to make them jump out.

> On remarque l'analogie entre la cuisson des grenouilles et la pression économique et médiatique mise sur la France. L'ensemble est assez provocant.

Can we avoid escalation ?
What if the attacker has little worth hitting ?
Yet the will to retaliate is more credible for cyberspace
A good defense adds further credibility

admin dit :
8 juillet 2011 à 10:00

1.6 Chapter four Why the purpose of the original cyberattack matters

Error
The attribution may be correct, but the presumption that the attack was a deliberate first strike by a state may not be. The attacker's command authority may not realize it has, in fact, been attacked. the attack may have been an accident. Or the attacker may view the event as an act of retaliation, even if it is not. the following paragraphs examining these cases.

Oops
The attack could actually be an accident or, less defensibly, may have been a minor flick that accidentally crossed a threshold.

No, you started it
Attackers who believe themselves to be righteous retaliators may be incorrect in their self-assessment (e.g., their attribution was bad), correct (e.g., the target's leadership was unaware that it had attacked), or oversensitive.

Rogue operators
An attack could come from within state organs but not from the state. the instruments of cyberattack are neither so enormous as to require national command authority nor so obvious as to subject their use to state veto. Even the fact that intelligence for the attack was collected under official auspices does not prove the attack was authorized: Intelligence preparation of the battlefield may have taken place as contingency for cybercombat at a later time or for combat using other means. Intelligence could have seeped to the actual attackers, who could be rogue bureaucrats, organized criminal entrerprises, coteries of well-connected hackers, or superpatriots.

> C'est amusant de voir que l'auteur appelle superpatriot quelqu'un qui n'obéit pas aux ordres. Nous aurions préféré la définition de « over zealous », trop zélé. Comment peut on être trop patriote ? La réponse réside sans doute dans les grandes écoles françaises qui préparent savament leurs élèves à être les valets du capitalisme anglo-saxon.

The command and control problem

Coercion
The biggest difference between coercion in real space and cyberspace may be one of credibility. If a bully rolls thousands of tank up to your border and announces its desire that you accommodate its interests, you may well consent without forcing him to demonstrate that the tanks are capable as they look. The same credibility calculus does not work in cyberspace. You may be entirely unsure of what a cyber attack may do to your economy and society because you are unsure of how capable the bully is and how vulnerable you are.

Force
Cyberattacks on a target's military and related systems are usually meant to weaken the target's ability to respond to crisis. A large, successful attack may retard the target's ability to wage war ; if the target's military deployment can be delayed long enough (e.g., after everything has been decided and after the aggressor's forces have dug in for defense), the target's military intervention may be deemed pointless. This may well be the key cyber risk.

In such circumstances involving the United states, retaliation would be no higher than the fourth issue on the President's plate. First would be determining wether war were, in fact, imminent – how soon and by what means. Second would be recovering the posture of the affected military units. If an attack were deemed inevitable, the highest priority would be to restore as much capability as quickly as possible to be ready against the hour or day of the attack (e.g., favoring patch and recover over deep-cleaning). Third would be conveying readiness if the fact and timing of the attack appeared contingent on how much damage through the cyber attack had caused. The target should try to convince the attacker that damage had been minimal and was being repaired quickly.

> On remarque ici que l'enjeu, le coeur de la cyberdissuasion sont associés à une problématique de disponibilité et de maintenabilité des matériels.

(…) A variant motive is to use attacks to make citizens lose faith in the target's government. Yet (1) only a foolish government would guarantee that it could defend private systems from cyberattacks; (2) faith in the U.S government rose after the September 11th attacks, largely because in time of crisis, people need to have faith in the goverment; and (3) advanced societies can function quite well, even when large majorities have no faith in the people who happen to run the government.

> On remarque ici qu'un gouvernement qui protègerait des systèmes privés est considéré comme fou (foolish). Ainsi on voit bien ici également, que cette dichotomie public, privé, remarquée plus haut a pour objectif la séparation des domaines liés à la sécurité, à la protection qui ressortent normalement de l'exercice régalien du pouvoir par l'Etat. En d'autres termes loin d'être une folie, la protection des systèmes privés par une organisation gouvernementale est très souhaitable pour garantir la disponibilité des services pour la population, contrairement à ce qui est dit dans ce document.

admin dit :
9 juillet 2011 à 8:55

1.7 Chapter five A strategy of response

Should the target reveal the cyberattack ?

When should attribution be announced ?

Should cyberretaliation be obvious ?

Is retaliation better late than never ?

Retaliating against state-tolerated freelance Hackers

What about retaliating against cne ?

Should deterrence be extended to friends ?

Should a deterrence policy be explicit ?

Can Insouciance defeat the attacker's strategy ?

Confrontation without retaliation

The attacker's perspective

Signaling to a close

admin dit :
9 juillet 2011 à 9:45

1.8 Chapter six strategic cyberwar

A campaign of cyberattacks launched by one entity against a state and its society, primarily but not exclusively for the purpose of affecting the target state's behavior, would be strategic cyberwar.

The purpose of cyberwar
States could find themselves at cyberwar in one of two ways: through deliberate provocation or through escalation. A cyberwar could arise deliberately, from one state's belief that it can gain advantages over another by disrupting or confusing the latter's information systems (akin to strategic air attacks in World War II). a cyberwar might also start as escalation and counterescalation in a crisis take on lives of their own (more akin to the mobilization contest of World War I). In either case, the onset of cyberwar means that primary deterrence has failed. That noted, however, secondary deterrence – the ability to establish do-not-cross lines – may still succeed.

(…)
One objective that cyberwar cannot have is to disarm, much less destroy, the ennemy. In the absence of physical combat, cyberwar cannot lead to the occupation of territory. It is almost inconceivable that a sufficiently vigourous cyberwar can overthrow the adversary's government and replace it with a more pliable one.

The plausibility of cyberwar

The limits of cyberwar
Casualties are the chief source of the kind of war weariness that causes nations to sue for peace when still capable of defending themselves – but no one has yet died in a cyberattack.

The conduct of cyberwar

Cyberwar as a warning against cyberwar

Preserving a second-strike capability
Attackers can, however, take steps to retard victim's efforts to make themselves less vulnerable, such as the following:
- Induce errors that look as though they could arise from software failures and transient conditions, rather than from attacks as such.
- Find ways to probe the targeted system for a reaction that is less likely to induce changes in the system as a response (defenders are less likely to make radical changes if they believe they have defeated such probes).
- Attack system-specific vulnerabilities rather than generic vulnerabilities (the latter, when patched, make many systems harder to attack again).
- Seek out who are unlikely to share their experiences with others; this way, a given exploit may be used again on another target.
- Use exploits that are likely to become obsolete and hence useless soonest (those with later use-by dates can be saved for latter contingencies).
- Take advantage of the sort of vulnerabilities that only a painstaking search can uncover. This is one

advantage of a supply-chain attack on software or hardware: It forces a thorough review of many components. Code that has been implanted months or years previous may have similar advantages.
- Find attacks that are relatively insensitive to simple countermeasures, such as disconnecting systems that really should not have been connected in the first place.

Sub-rosa cyberwar ?
Cyberwar is unique in that the public need not know it is taking place – may not know what the problem is or, indeed, wether there is any problem at all. Factors other than cyberwar (e.g., error, accident) can be adduced to explain visible disruption – up to a point. Thus, a sub-rosa cyberwar is not impossible. But would it be worthwhile ?

A Government role in defending against cyberwar

Apart from protecting its own systems, the most obvious ways that government can defend against cyberwar are indirect: sponsor research, development, and standard creation in computer network defense.

> A l'évidence, ce genre de propos, comme précisé plus haut ne peut être qu'un leurre. En effet comment peut on concilier la prévention des attaques des chaînes d'approvisionnement et l'abandon de la protection, l'autogestion des systèmes privés.

Managing the effects of cyberwar

Terminating cyberwar
War strategies are ultimately about war termination. cyberwar, as noted, is highly unlikely to be terminated because the adversary has been disarmed (much less overturned) by force. such wars are more likely to end by exhaustion or by concessions. Unfortunately, the longer wars go on, the less they are about their original aims and the more they are about themselves (e.g., revenge and, less irrationally, the mutual desire of each side to ensure that it is secure from the other).
Cyberwars presents and additional and compelling challenge: How can one tell that the other sides has, in fact, stopped its attacks ?
Consider three war termination paths: negotiation leading to termination, tacit de -escalation, or petering out.

admin dit :
9 juillet 2011 à 12:46

1.9 Chapter seven Operational Cyberwar

Operational cyberwar consists of wartime cyberattacks against military targets and military related civilian targets. Even if this does not constitute raw power, it can be a decisive force multiplier if employed carefully, discriminately, and at precisely the right time.

(…) Cybersupremacy is impossible because cyberspace is not a unitary domain. Both organizations can simultaneously keep each other off their own networks. In practice, hackers do get into other people's networks. Unfortunately, the idea that someone « owns » another network if he or she can make its machines obey his or her instructions abuses the concept of ownership. Ownership implies exclusivity. If nothing else, outside hackers cannot claim physical control, and physical control dominates all other forms of control. Owners can physically add or remove machines from a network and can install software directly. If worse comes to worst, owners can discard and replace systems.
(…)
The remainder of the chapter discusses some of the operational challenges of operational cyberwar. Cyberwar can play three key roles: it might cripple adversary capabilities quickly, if the advesary is caught by surprise. It can be used as a rapier in limited situations, thereby affording a temporary but potentially decisive military advantage. It can also inhibit the adversary from using its systems confidently.

Cyberwar as a bolt from the blue
Cyberattacks are about deception, and the essence of deception is the difference between what you expect and what you get: surprise.
(…)Many military surprises appear in retrospect to have succeeded because attackers found unexpected ways to neutralize disadvantages that the victim thought should have precluded action. In this case, it is difficult to think of how a cyberattack on civilian infrastructure would reduce the victim's military efficacy or its top-down command and control (unless military operations could not be carried out if civilian telecommunications were down). Starting at the strategic level also threatens strategic retaliation from the outset (possibly trumping on-the-ground gains). this surprise, then appears to be irrational. However, as Richard Betts has observed, « [a]pparently irrational behavior is one of the most important elements in several past surprise attacks. »

Dampening the ardor for network-centric operations

Attacks on civilian targets

Disrupting or corrupting communications or transportation systems may help cripple military operations. Hitting civilian telephone switches may interfere with a military's command and control; even if military systems are separate, diasabling other systems may hinder military mobilization.

> On remarque l'inextricabilité des communications militaires et des communications civiles, notamment dans le cadre d'une guerre civile, ou d'un contrôle médiatique.

Organizing for operational cyberwar
(…)
Yet those who prepare and conduct operational cyberwar will have to inject the intelligence operative's inclinations into the military ethos. These inclinations include seeking discrete rather than wholesale effects; the ability to wait patiently; an intuitive understanding that one is operating on the other guy's turf; a healthy wariness of deception, indirection, and concealment; and; yes, a willingness to abandon attack plans to keep

intelligence instruments in place.

Conclusions
Living in an information age does not make operational cyberwar the be-all and end-all of military operations. If stretched that far, it could end up becoming nothing. Operators should also recognize that the best cyberattacks have a limited « shelf life » and should be used sparingly. If it is recognized for the rare and special thing that it is, operational cyberwar may have a few interesting roles to play.

admin dit :
9 juillet 2011 à 14:16

1.10 Chapter eight Cyberdefense

This monograph has strongly implied the importance of defending cyberspace thus far, largely because deterrence appears to be too problematic to offer much surcease from cyberattacks. Even DoD, which does have an offensive cyberwar mission, will likely spend and need to spend far more on defense than on offense – of which the ability to retaliate, hence deter, can only be part. A similar tilt is likely to characterize the U.S. Air force as well, despite its global strike role.

(…) This discussion is limited to national defense systems, which are mostly but not exclusively military. Although many of the distinctions between military and nonmilitary systems are familiar, it may help to briefly reiterate three that are relevant to this chapter:
- Militaries hav real enemies that wih to diminish them; other organizations have rivals but are more likely to be attacked for opportunistic or indirect reasons.
- Military generally do not have customers; thus, their systems have little need to be connected to the public to accomplish core function (even if external connections are important in ways not always appreciated).
- Militaries are ordinarily on standby; they earn their keep by being prepared for extraordinary circumstances.

> On voit bien ici que le premier point est une négation de l'existence d'industrie de défense, qui ont un statut privé, mais participent à des activités classifiées et stratégiques, que par extension toute industrie stratégique est exposée à des menaces auxquelles pourraient être exposés les militaires, notament dans le cadre d'une attaque de chaîne d'approvisionnement. Ce qui implique que le document tend à prolonger le leurre mis en place dans les années 80 et qui a précipité l'occident dans une activité frénétique d'externalisation et de privatisation qui allaient contre l'intérêt de ses Etats.

The goal of cyberdefense
Robustness – the ability to extract as much military power from systems under stress as from systems free of stress – is no less important for information systems than it is for any other military system.(…)
REcoverability is a key aspect of robustness – the ability to get some systems to cover for those that have been damaged while the compromised portions are being isolated, diagnosed, fixed, checked out, and returned to

service.

> On remarque ici que l'enjeu repose sur des caractéristiques de soutenabilité du matériel et des logiciels, soutenabilité qui se caractérise par une meilleure disponibilité, une meilleure maintenabilité, une meilleure fiabilité. C'est précisément ici que les systèmes propriétaires comme Microsoft Windows à code source fermé sont défaillants.

A simple analogy would suggest the same for cyberspace: Invest in robustness, protect core information-system capabilities, train to fight with degraded and suspect information systems, and emphasize the ability to reconstitute smartly following an attack.

(…)
After robustness, the next critical goal is system integrity: The system does what its operator wants it to do, and does not do what its operator does not want it to do.
(…) Although warfighters often have no choice but to trust their fighting machines, trust is more likely to be discretionary with information systems. An information system that is mistrusted but otherwise functional is just not very functional.

The last goal is confidentiality, the ability to keep secrets, not only those integral to the military's own operations but secrets others (such as the intelligence community) have entrusted to it.

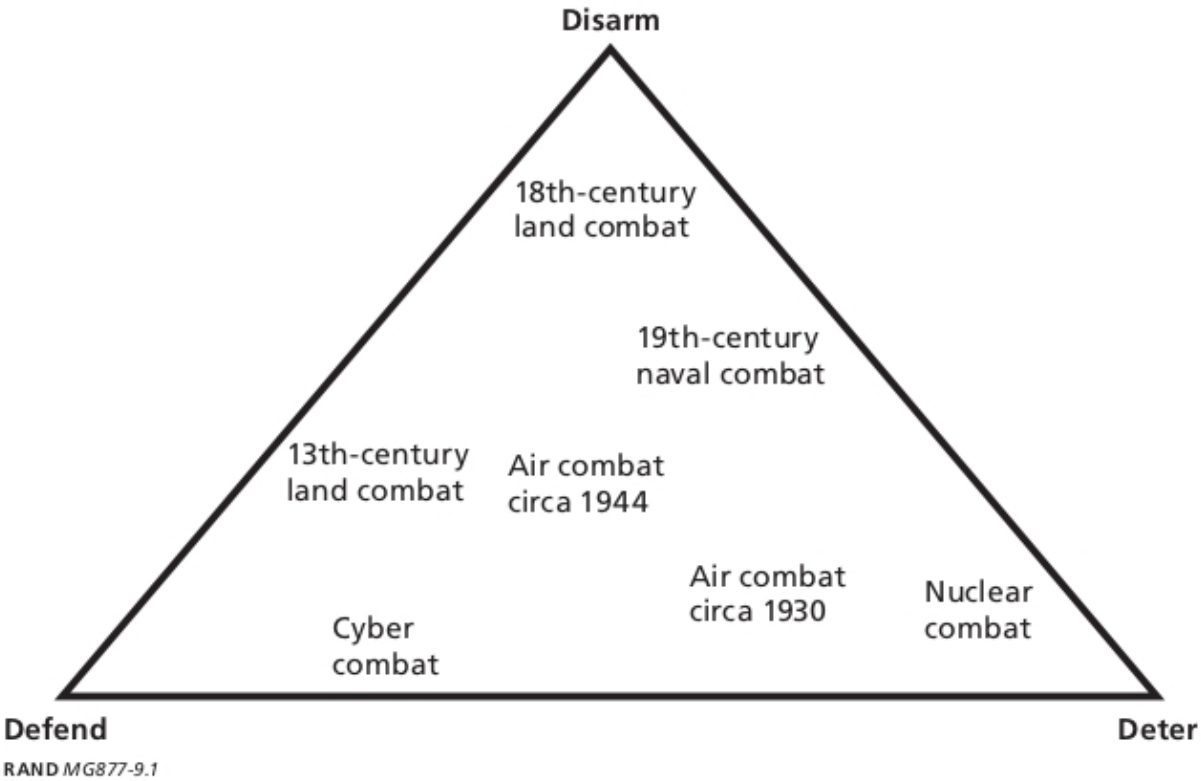
Architecture
US military achitecture is multilayered, consistent with the discussion on cores and peripheries in Chapter two. It runs unclassified networks (the NIPRnet) that can access the internet, support everyday communications of warfighters, and link DoD to its broader support community. It runs classified networks (SIPRnet) for command and control and the protection of sensitive information; such systems are air-gapped from the rest of the world. Finally, it runs various subnetworks at higher levels of classification to handle the most sensitive intelligence data.
(…)
One way to envision the proper distinction between NIPRnet and SIPRnet is to think of the former as the conduit for influence, liaison, and learning and the latter as a conduit for command and control (plus intelligence in yet more secure networks).

Policy
Strategy
Deception
Red Teaming

admin dit :
10 juillet 2011 à 6:35

1.11 Chapter 9 Tricky terrain

Figure 9.1
Where Various Forms of Combat May Fit in the Deter-Disarm-Defend Triangle



In traditional land combat, for instance, the emphasis was on disarming the enemy in combat. relying on defense generally did not work very well (The maginot line being a prime example), and deterrence by threat of punishment generally required a disarmed or poorly armed ennemy (Sherman's march through Georgia, for example). In late medieval times, when castles were strong and artillery had yet to be introduced, the optimal point was closer to the defense apex of the triangle. In naval combat, the contest was historically over freedom of navigation; defense played a very small role (except at the tactical level, in terms of ship design). Yet there were vigorous debates between disarming (in terms of a « fleet in being ») and deterrence by punishment (in terms of « commerce raiding »). Early observers of air warfare believed cities to be impossible to defend and were pessimistic about disarming invasion fleets, and so focused on deterrence. As World War II commenced, populations evidenced a more stalwart attitude toward air attacks; disarming the Luftwaffe proved possible in the Battle of Britain, but ground-based air defense was often futile. the optimal point moved toward the middle of the triangle. In the nuclear age, especially when expressed int terms of missiles, defense was nearly

impossible, disarming (« Counterforce ») was a second-strike consideration, and so the preimary emphasis was on deterrence (« countervalue »).

(…) Can the United States avoid cyberdeterrence and cyberwar altogether ? Perhaps there is a foe so foolish as to attack the world's strongest military power by causing great annoyance to its society (perhaps by turning off everyone's light, were it possible) and, in effect, asking: What are you going to do about it ? The United States should probably be able to answer that query.

> On pourrait résumer l'objectif du document à ce simple paragraphe. L'auteur devrait rajouter « Now let's have a beer ! » ou en français « Allé Gros, paye moi une bière ! ».