APPLYING THE PRINCIPLES OF WAR TO THE CYBER SECURITY DOMAIN

Commander Subhash Dutta, Indian Navy (Retd)
04 May 2021

Anyone who has spent a significant period of time within the Information Security (InfoSec) industry would recognise the industry's felt need to reinvent itself at regular intervals. This author has always found this to be a rather defeatist approach as the impression that it creates is that InfoSec professionals are in a constant tail-chase, while the attackers always have an upper hand. However, a dispassionate assessment of security technologies and their core functions would lead one to realise that nothing really has changed. The attackers have always been after data/information that can be monetised, and the defenders have always been trying to prevent this and protect the sought-after data/information.

While the technologies underpinning IT-infrastructure have advanced rapidly over the last few years, the underlying feature — the ability to rapidly process and consume information — has remained the same. After their initial attempts to attack information systems, the focus of attackers has always been the information rather than the systems that create, store, or process this data. Therefore, it stands to reason that while our defensive tools and processes may change to keep up with newer systems or technologies, the basic principles must remain the same.

This article is a consequence of numerous discussions with professionals chartered with keeping their IT infrastructure and users safe — these professionals typically bear the designation, Chief Information Security Officers (CISOs) —– regarding specific threats. From the earlier generations of "rootkits" — hidden malware[1] that incorporates a number of tools, ranging from programmes that allow hackers to steal passwords, to modules that make it easy for them to steal credit card or online banking information or enable them to subvert or disable security software and track the keys that are tapped on a keyword in order to steal personal information)[2] — the industry transitioned to "Advanced Persistent Threats" (APTs) — *"in which an unauthorised user gains access to a system or network and remains there for an extended period of time without being detected"*[3] — and now the conversation of CISOs is peppered with a generous sprinkling of ransomware.[4] If one were to consider the basic functioning of these classes of malware, one

[1] Malware is a *"portmanteau"*, a word coined from the combination of the words malicious and software, commonly used within the InfoSec community
[2] Dan Rafter, "What is a rootkit? And How to Stop Them", NortonLifeLock Inc
https://us.norton.com/internetsecurity-malware-what-is-a-rootkit-and-how-to-stop-them.html
[3] Nate Lord, "What is an Advanced Persistent Threat? APT Definition", 11 September 2018,
https://digitalguardian.com/blog/what-advanced-persistent-threat-apt-definition
[4] Josh Fruhlinger, "Ransomware Explained: How it Works and How to Remove it", CSO Online, 19 Jun 2020.
https://www.csoonline.com/article/3236183/what-is-ransomware-how-it-works-and-how-to-remove-it.html

would find that there are remarkable similarities amongst them. The California-based American multinational technology conglomerate, Cisco Systems, Inc, commonly known simply as "Cisco", defines an APT as "*processes (that) require a high degree of covertness over a long period of time*".[5] This is markedly similar in capability to a rootkit, which hides the existence of malware by hooking and altering the 'requests made to' and the 'responses received from' a remote server's "Application Programming Interface" (API), which is *"the part of the server that receives requests and sends responses"*.[6]

However, if one were to tell them that instead of chasing threats, which will be constantly evolving, CISOs must focus on their risks (where is their critical data, who has access to it and where is it moving) one would probably get a politely thoughtful stare and then the conversation would rapidly change back to "but what can your product do against ransomware?"

Needed: A Shift in Thinking so as to Simplify Security.

So, what is required to change the mindset? The first and foremost need is to uncomplicate security. This is not very hard to do but it has never received the focus that it deserves. InfoSec professionals the world over, are find themselves drowning in a veritable deluge of information — something that is commonly referred to as "information overload. As a consequence, they suffer greatly from "alert-fatigue". Triaging incidents to take on the most dangerous threat considering the criticality of the system being attacked is virtually impossible when facing up to 900 million events per day[7] (something that most Security Operation Centres face).

IT administrators and InfoSec professionals are in a daily battle against attackers who are constantly on the lookout for low hanging fruit. The most common adage in the InfoSec community is that while the security professional must ensure that every single door and window is secured, the attacker has to find just one tiny crack or hole. Thus, it is not a question of "whether" but rather, of "when" an organisation would be successfully attacked and lose data.

If at least a modicum of succour is to be provided to these beleaguered InfoSec professionals, the best way would be to reduce the number of dashboards/consoles that they need to monitor. A single "endpoint security solution"[8] that provides advanced protection against threats emanating from outside while also preventing movement of data to an unauthorised entity would cover several different and discrete (independent) security products that are currently in use — for example, antimalware, patch management, Data Leakage Prevention (DLP), device-hardening, host-based firewall/Intrusion Detection/Protection System (IDS/IPS), application control, etc.

---

[5] "What Is the Difference: Viruses, Worms, Trojans, and Bots?", Cisco, 14 June 2018, https://tools.cisco.com/security/center/resources/virus_differences#APT

[6] Petr Gazarov, "What is an API", FreeCodeCamp, 19 Dec 2019, https://www.freecodecamp.org/news/what-is-an-api-in-english-please-b880a3214a82/

[7] This is a representative figure. Sequretek IT Solutions SOC ingests around 800 million events per day from almost 3500 devices spread across its more than 60 clients.

[8] https://sequretek.com/wp-content/uploads/2018/10/EDPR_Datasheet.pdf

Adapting the "Principles of War" to InfoSec.

The second most important factor is to fight this menace much as a nation would fight a war. Nation-states have been fighting wars for centuries and have distilled from the experience they have gained at such a high cost — in terms of the human lives lost and the property and infrastructure destroyed — some basic principles that lead to victory and whose neglect pretty much assures defeat. Renowned strategic thinkers, such as Sun Tzu[9], Chanakya[10], Machiavelli[11], Clausewitz,[12] amongst several others, have outlined these principles — "Principles of War" as they are termed — that have successfully stood the test of time. Even though there are some variations that cater to individual national peculiarities and the military doctrines that flow from these individual circumstances, there is, nevertheless a very remarkable degree of commonality that stretches across both, time and space.

The British enunciated ten Principles of War after their experience within the Great War (a.k.a. the First World War) that were the outflow of the remarkable work done by the British general and military theorist, JFC Fuller.[13] With only some minor variations, these principles have been adopted by the contemporary British armed forces, as also by those of most Commonwealth Sates. The current Principles of War stipulated in the UK Defence Doctrine[14], which have also been adopted (or slightly adapted) by the North Atlantic Treaty Organisation (NATO) in its *"Principles of Allied Joint and Multinational Operations"*[15] are:

(1) Selection and maintenance of the aim (adapted by NATO as *"Unity of Effort" and "Definition of Objectives"*)
(2) Maintenance of morale
(3) Offensive action (adapted by NATO as *"Offensive Spirit"* and *"Initiative"*)
(4) Security
(5) Surprise
(6) Concentration of force
(7) Economy of effort
(8) Flexibility (adapted by NATO as *"Freedom of Action"*)
(9) Cooperation (adapted by NATO as a "characteristic" rather than a "principle", and described as *"Multinationality"*)
(10) Sustainability (adapted by NATO as a "characteristic" rather than a "principle", and described as *"Perseverance"*)

---

[9] Joshua Mark, "Sun-Tzu", World History Encyclopaedia, 09 Jul 2020. https://www.worldhistory.org/Sun-Tzu/
[10] *Wikipedia*, s.v. "Chanakya", last modified 28 Feb 2021, 07:32, https://en.wikipedia.org/wiki/Chanakya
[11] Cary Nederman, "Niccolò Machiavelli", Stanford Encyclopaedia of Philosophy, 28 May 2019. https://plato.stanford.edu/entries/machiavelli/
[12] Jordan Lindell, "Clausewitz: War, Peace and Politics", E-International Relations, 26 Nov 2009. https://www.e-ir.info/2009/11/26/clausewitz-war-peace-and-politics/
[13] *Wikipedia*, s.v. JFC Fuller, last modified 15 Mar 2021, 16:58, https://en.wikipedia.org/wiki/J._F._C._Fuller
[14] UK Ministry of Defence, "UK Defence Doctrine, Annex 2A", Nov 2014, https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/389755/20141208-JDP_0_01_Ed_5_UK_Defence_Doctrine.pdf
[15] Allied Joint Doctrine (AJP-01), Edition E Version 1, February 2017, 1-13, https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/905877/20200728-doctrine_nato_allied_joint_doctrine_ajp_01.pdf

Particularly germane to this article is the one striking variation that NATO's listing incorporates (as compared to the UK's list) — probably as a result of the former's long experience in dealing with its quarrelsome and often fractious constituent members. This is the principle of *"Simplicity"*. Indeed, the central underlying message of this entire article is precisely this — a plea for "Simplicity".

That having been said, it is not merely possible, but would be hugely beneficial to use these principles (drawn from the UK's Defence Doctrine) to the domain of Information Security and to thereafter devise strategies and tactics in conformity with these principles.

Selection and Maintenance of Aim. This is the first and preeminent principle and guides all subsequent actions within any organisation, military or civilian. Organisations must have a singular and unambiguous aim — the protection of critical data to ensure continuation of business operations. This must be communicated clearly to the InfoSec team. Decisions taken in pursuance of this principle will, thereafter, govern all other actions.

Maintenance of Morale. Security professionals are confronted by a deluge of information comprising an incredibly high frequency of threat- and attack-alerts, which causes an information-overload at individual and institutional levels, resulting in "alert fatigue". All too often, the actions that InfoSec personnel take to protect the assets of their organisations go unnoticed and hence unrecognised. This leads to a lowering of morale, which, when coupled with alert-fatigue, makes for quite a deadly cocktail. It is of utmost importance that InfoSec personnel are perceived as frontline "warriors" and acknowledged as such, and that their efforts are publicly rewarded. While monetary rewards do provide some satisfaction, peer recognition and regular feedbacks have been known to produce far better results. Simultaneously, reposing trust in security partners will provide additional gains.

Offensive Action. A series of activities that enable these InfoSec "warriors" to seize the initiative, gain an upper hand, and maintain momentum over attackers ensures will, taken in aggregate, almost invariably ensure the protection of the security of an organisations' critical data. Allocation of resources in terms of talented personnel and appropriate security systems is essential. It is equally critical for InfoSec team leaders to be empowered to take actions to fend off attacks with minimal requirement to process approvals through a convoluted chain of command. On the other hand, while the people on the ground will always demand more manpower and resources, it is the higher "C-level" authorities or CxOs[16] as they are also known, who must retain a clear idea of the strategic picture and it is they who must frame long-term priorities in terms of the allocation of human and material resources. To do so wisely, they must be crystal clear about the criticality of individual systems and be able to identify those that need

[16] In a commercial organisation such as a registered company, senior executives charged with ensuring that the company stays true to its pre-set plans and policies, are often given titles that beginning with the letter "C", standing for "Chief" and ending with the letter "O" for "Officer." Examples are "Chief Executive Officer" (CEO), "Chief Financial Officer" (CFO), "Chief Information-Security Officer" (CISO), etc. These are frequently collectively known as "C-Suite" or "C-level" executives. Given the proliferation of these titles, they are collectively referred to as "CxOs"

higher protection and, therefore, require a more generous allocation of resources. If these critical systems fail (which is why they are known as "critical" systems in the first place!), everything else will collapse.

Security. The application of this principle must always ensure that one's "base', or "home turf" or "parent company" is secure. This then provides for an operating environment that gives freedom of action, when and where required, to achieve objectives. On the other hand, most security controls are considered an inconvenience and internal users frequently attempt to circumvent them, thereby achieving apparently impressive but potentially disastrous and artificially high speeds in terms of operational processes. Management must, therefore, repeatedly send out a clear and unambiguous message that the security controls in place do not imply any mistrust in the employees, but rather, seek to provide a safe a secure environment within which these very employees can be productive. Even if this means biting the bullet from time to time, InfoSec teams must be empowered to take urgent protective action when required.

Surprise. From an attacker's perspective, surprise is a desirable consequence of sowing confusion and inducing panic amongst defenders by deliberately or incidentally introducing the unexpected. Obviously, InfoSec professionals must guard against being surprised by attackers. To preclude surprise attacks from being effective, the most important ingredient in the armoury of the InfoSec team is up-to-date and comprehensive "intelligence". The "Who" component is important, but significantly less so than being able to predict the "What" component, so that the always-unknown nature of the "When" component does not throw the defenders completely out of gear. The enormous value of knowing just what is out there is quite akin to the value conferred, within the maritime space, to a defender who possesses a high degree of "Maritime Domain Awareness" (MDA). While it is critical to know what to look for, this itself depends upon how thoroughly one is aware of just "what" is out there. Thus, threat- and malware intelligence is essential for the development of a picture that provides a holistic view of the hostile environment. Any blurring or blindness of such a view enables attackers to retain the element of surprise and, hence, initiative. If intelligence — it cannot be stressed enough that a prerequisite of "specific" intelligence is "general" intelligence — is missing or inadequate, the best that an InfoSec team can be expected to do once the organisation has been allowed to be taken by surprise, is to be reactive one with a general lack of direction. This is a situation that is not only disastrous in the short run, but is also deeply frustrating in the long run.

Concentration of Force. In military terms, this involves decisively applying superior fighting power (physical, intellectual, and moral) to realise intended effects, when and where required. For InfoSec warriors, it is essential that they do not spread themselves too thin and attempt to do everything simultaneously. Meticulous planning is required by the CISO to analyse the critical components that would require his or her prioritised attention, align personnel to these established priorities, and, equip them with the requisite tools with which to fight both, localised outbreaks and more general attacks.

Economy of Effort. This principle invokes the judicious exploitation of resources to achieve the objective. Activities pursuant to this principle flow from the previous one on "Concentration of Force". The InfoSec team of a CISO who attempts to do everything will very

probably end up doing nothing. Resources will always be in short supply, security systems may not be optimally configured, personnel may lack training, or the time available to respond and recover may not be adequate. InfoSec leaders will never have an option other than to prioritise. Prioritisation certainly leads to economy of effort but the decision as to what to prioritise and when to do so, must be based upon a continuous and dynamic evaluation of possible threats — as revealed by past attacks that have been dealt with elsewhere (or else-when) through preventive deterrent means, or preventive approaches, or curative actions. CISOs must be trained to plan for contingencies and ensure that process delays are ironed out and resources are not only available to meet a given requirement but can be switched smoothly should a higher priority threat be identified.

Flexibility. As just outlined above, the principle of "flexibility" connotes the ability to change rapidly but smoothly to meet new circumstances. Attackers may not always follow a set pattern; they will often look for targets of opportunity and a vulnerable internet-facing resource might invite their unwelcome attention. The only real way to attain "flexibility" is through well-rehearsed drills and simulations. Of course, "flexibility" also requires that greater autonomy be accorded to personnel who need to act quickly to mitigate an emergent threat that carries a greater risk of compromise of information. Resilient business operations during an ongoing attack will only be possible if responses are not rigid, but instead, agility and adaptability are incorporated in security operations.

Cooperation. Surprisingly, many organisations do not follow a structured and carefully implemented method of team-building, and the development of multiple levels of team leadership. Trust-deficits are a particularly ubiquitous flaw in far too many organisations. This is especially the case with start-ups, whose leadership assumes that by some divine method of osmosis, their own skills (especially skills that stood them in good stead in some past position or endeavour) will automatically result in a well-bonded team in which internal processes of cooperation and collaboration teamwork can be taken to be a given. This lack of managerial commitment and the concomitant investment of time, effort, and, most important of all, persistence, is the single biggest reason that so many InfoSec teams (and organisational management structures as a whole) do poorly. Cooperation is not just about being nice to one another. It also implies the sharing of dangers, burdens, risks, and opportunities in every aspect. It is this shared responsibility in terms of both, success and failure, that creates the sore of bonding that HR set-ups enunciate but seldom achieve. It is essential that the HR structure as well as the departmental organisations responsible for corporate communications and legal aspects be in complete sync with the InfoSec team. The flow of information between these various departments must be seamless and systems should be in place to exchange this information. Once again, this requires committed rehearsals — what the military calls "drills". A telling example of the risks of inadequate attention having been paid to the principle of cooperation is that of an employee who has left the organisation, but whose accesses to obscure repositories remain and are open to abuse.

Sustainability. Just as nations and militaries emphasise "sustenance" to ensure the ability to fight and preserve freedom of action, so must organisations enable their InfoSec teams by providing them with adequate and well-drilled resources to fight off determined attackers.

Investments in training and upgrading the skills of InfoSec warriors will pay handsome dividends when a serious attacker is encountered. This will also ensure that committed and capable resources remain with the organisation for a longer period — a feature that is in great demand in an industry with high horizontal mobility of personnel and consequent high rates of attrition within a given company or organisation.

Conclusion

Early malware activities were largely nuisance attacks, such as defacing or putting graffiti on an organisation's webpage. Present day malware attacks have become full blown cyber offences involving determined sophisticated attacks on critical infrastructures and sophisticated crimes. Not surprisingly an underground ecosystem has emerged to support the full malware lifecycle, which includes development, deployment, operations, and monetisation. This ecosystem has spawned a number of actors who specialise in key parts of the malware lifecycle, and, by providing their services to others, they obtain their share of the ill-gotten financial gains and rewards. Unfortunately for those charged with assuring information security, such specialisations markedly improve the quality of malware. For example, a contemporary attacker can hire the best exploitation-researcher to write that part of the malware responsible for remotely compromising a vulnerable computer. A wider example is that of the progression of ransomware.[17] It started off as simple data encryption, with payment of ransom being required for the decryption key. Organisations adapted to this by ensuring proper backups of critical data, rebuilt their systems, and then refused to pay ransom. The attackers then changed tack and exfiltrated data prior to encrypting it and now demanded a ransom to prevent the data from being exposed publicly. Organisations now protected themselves with ensuring that protective measures — such as encrypting data — were rigorously enforced while also opting for cyber risk-insurance. The attackers then again shifted their tactics and started informing clients and users whose data had been exposed that they would name and shame the compromised individuals and/or organisations!

An InfoSec organisation must be agile, and must be able to keep up with the continuously evolving techniques, tactics, and procedures of attackers, by building a robust databank comprising intelligence of threats and malware. Organisations, too, must do their part by supporting their InfoSec warriors by way of the provision of resources, capability, and technical advancement. Overall, there must be a concerted effort at reducing the complexity of security operations so as to reduce the degree of alert fatigue currently being faced in information-security operations.

About the Author:

Commander Subhash Dutta is a former Indian Naval Officer and an Adjunct Fellow at the National Maritime Foundation. He can be contacted at subhashdutta.nmf@gmail.com

[17] Kevin Savage et al, "The Evolution of Ransomware", *Florida State University*, 06 Aug 2015. https://its.fsu.edu/sites/g/files/imported/storage/images/information-security-and-privacy-office/the-evolution-of-ransomware.pdf