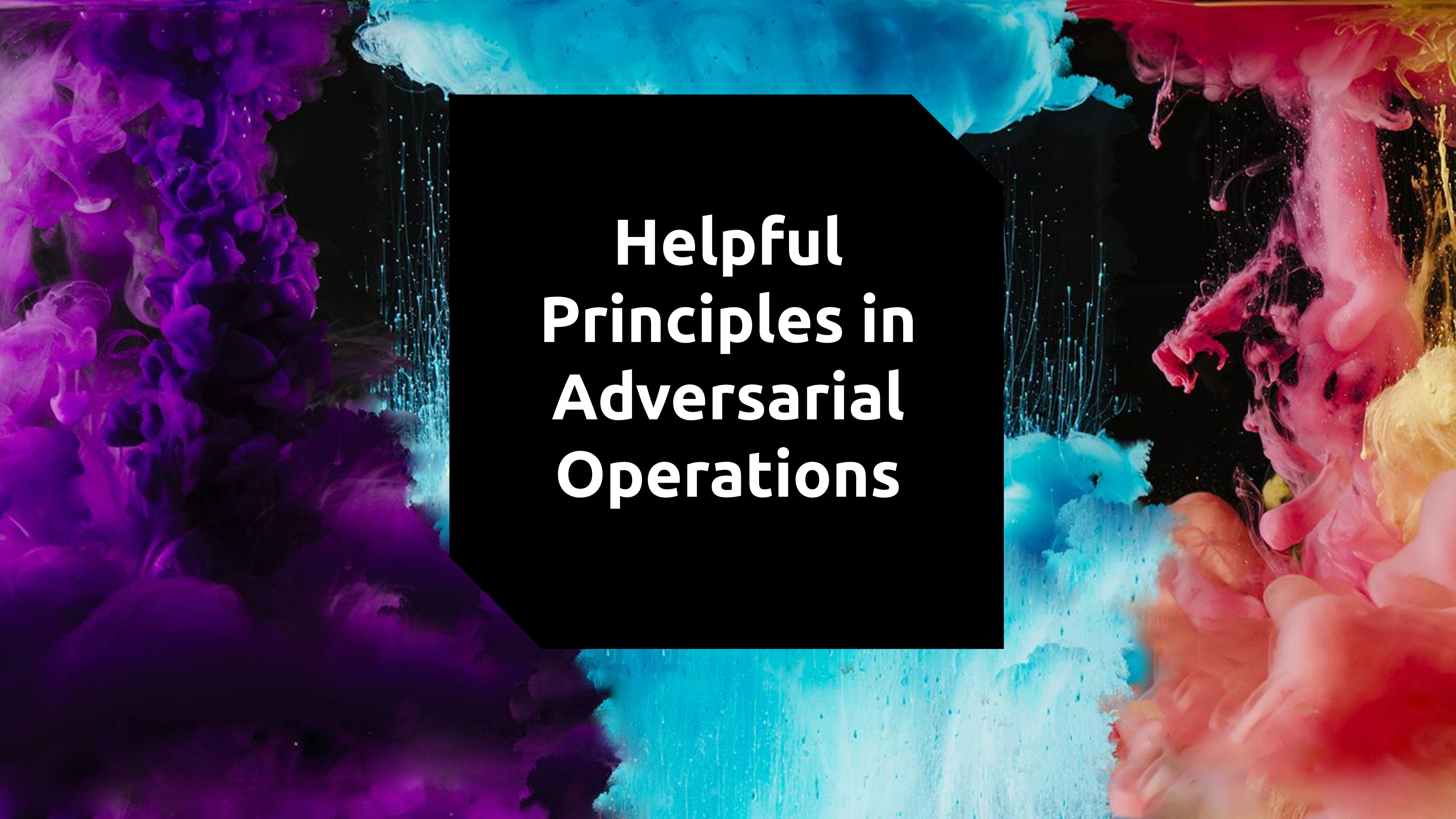


Helpful Principles in Adversarial Operations

Contents

1

About me

How did I get here?

2

Why principles?

Why should we use these?
How can these help?

3

The principles

What are they? How can we apply them? Tales from the syslog.

$ whoami

15 years of infosec (pentesting, red team, incident response)

8 years of multiple attack and defense competitions

Wrote a best selling infosec book

Currently an incident response lead

Writes a lot a lot at lockboxx.org

Disclaimers

- This is a theory talk
- Some of these are simple
  - I bring them up because they can be leveraged
- There are exceptions, these aren’t bullet proof
  - These are principles not laws
- There are many more principles, these are just some of my favorite

Where these principles come from

These principles have been borrowed and adapted from several great thinkers on conflict:

- Barton Whaley’s “Toward a General Theory of Deception”
- Barton Whaley’s “Practice to Deceive”
- Robert M Clark’s “Deception: Counterdeception and Counterintelligence”
- “Military Deception: Hiding the Real - Showing the Fake” by Mark Johnson and Jessica Meyeraan
- Matthew Monette’s “Network Attacks and Exploitation: A Framework”
- The CIA's "Development Tradecraft DOs and DON'Ts"
- Sun Tzu’s “The Art of War”
- The Checklist Manifesto

- .. mixed with years of my own practice and application and tailored specifically for computer based conflict

About Attack and Defense Competitions

Real time offense vs defense in a computer network.

Not exploit or memory corruption based - they are higher level in terms of red teaming vs incident response.

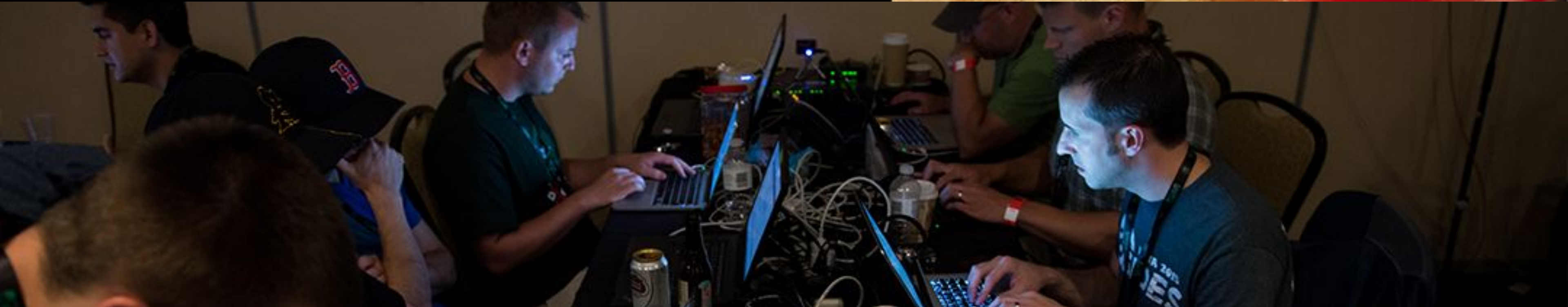
Very real world, similar to real cyber attack / incident, except condensed onto a very short timeline.

Offense vs Defense

Cyber security is asymmetric in terms of offense and defense.

There are fundamentally different strategies, tools, tactics, and even operations between cyber offense and cyber defense.

This means totally different approaches to the game. While they can learn and adopt a lot from each other, they are unique in their execution and goals.



What are the principles of cyber conflict we will cover?

1. Principle of **Deception**

2. Principle of **Physical Access**

3. Principle of **Humanity**

4. Principle of **Economy**

5. Principle of **Planning**

6. Principle of **Innovation**

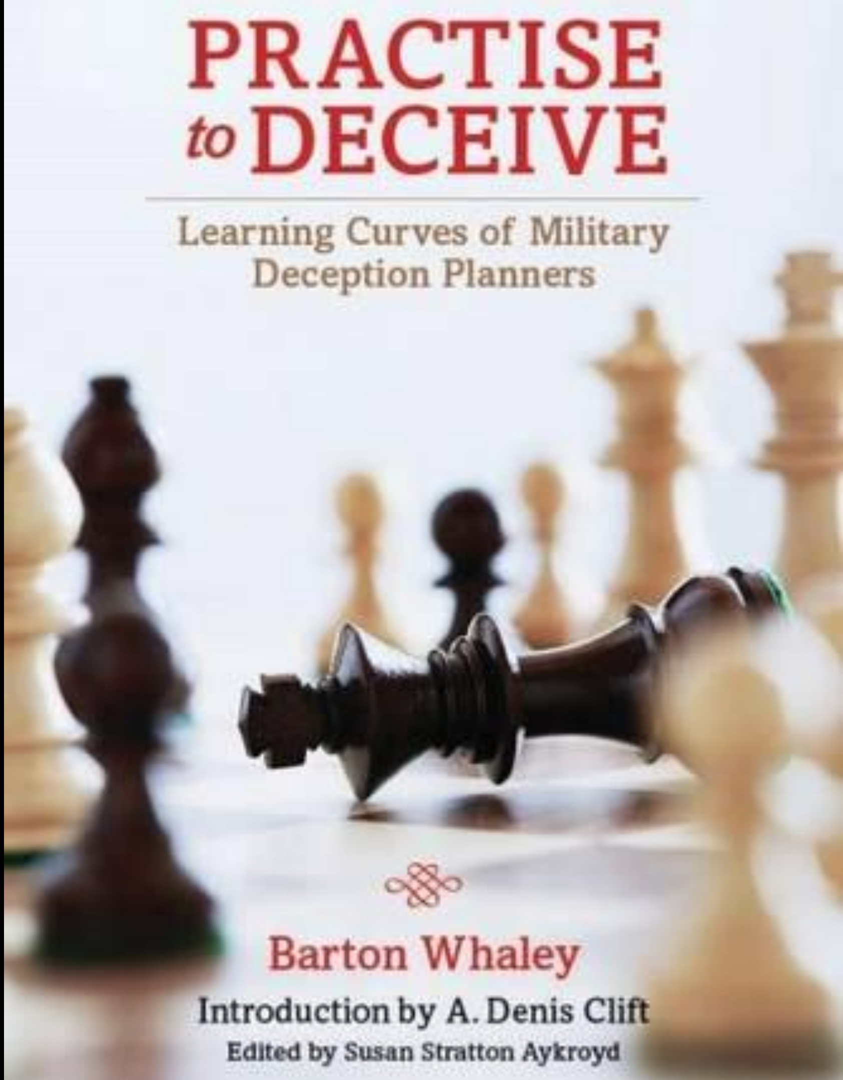
7. Principle of **Time**

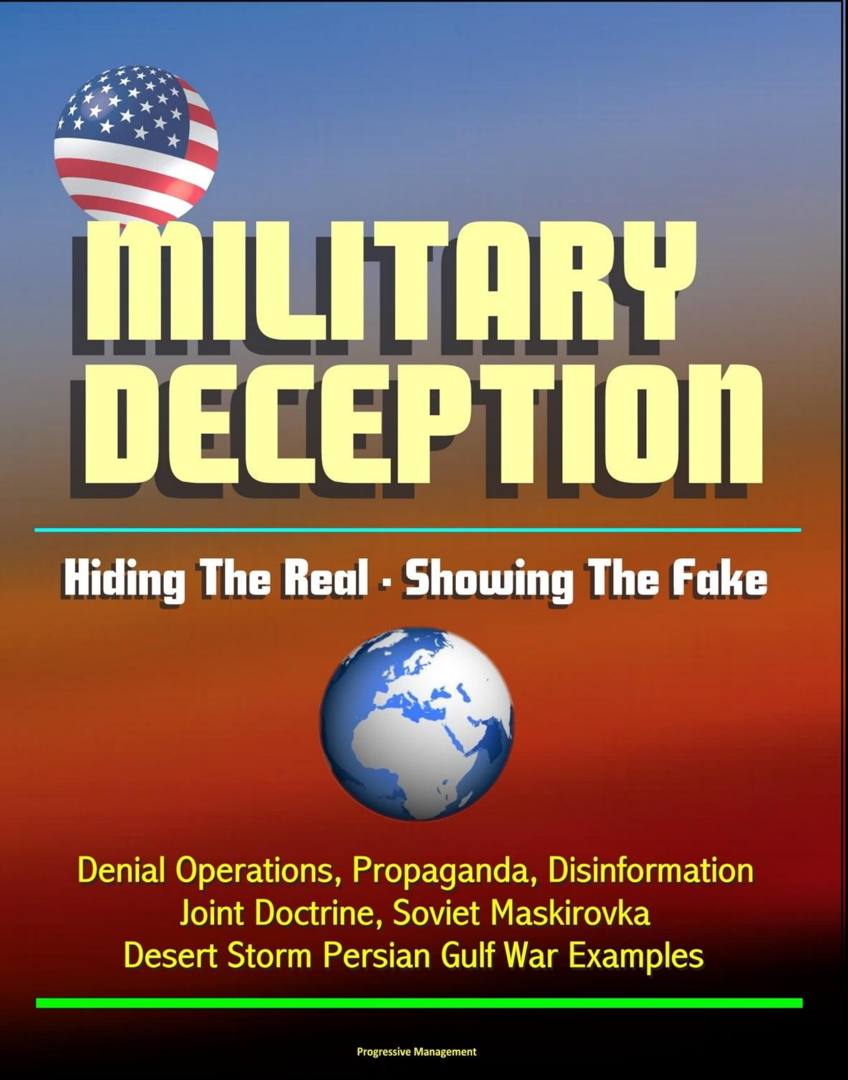
1. The Principle of Deception

States that the use of deception, such as obfuscation or showing fake data, will help us get an advantage over an opponent in a computer conflict.

> “All warfare is based on deception”
>
> - Sun Tzu

In computer security, both offense and defense relies on the other side not knowing their specific techniques, tools, and signatures. Or they would be trivial to deal with (block or bypass)


PRACTISE to DECEIVE
Learning Curves of Military Deception Planners
Barton Whaley
Introduction by A. Denis Clift
Edited by Susan Stratton Aykroyd



MILITARY DECEPTION

Hiding The Real · Showing The Fake

Denial Operations, Propaganda, Disinformation
Joint Doctrine, Soviet Maskirovka
Desert Storm Persian Gulf War Examples

Progressive Management

“Military deception is an umbrella term that includes both denial and deception. Denial **hides the real** and deception **shows the fake**.”, from **Military Deception: Hiding the Real - Showing the Fake** by Mark Johnson and Jessica Meyeraan

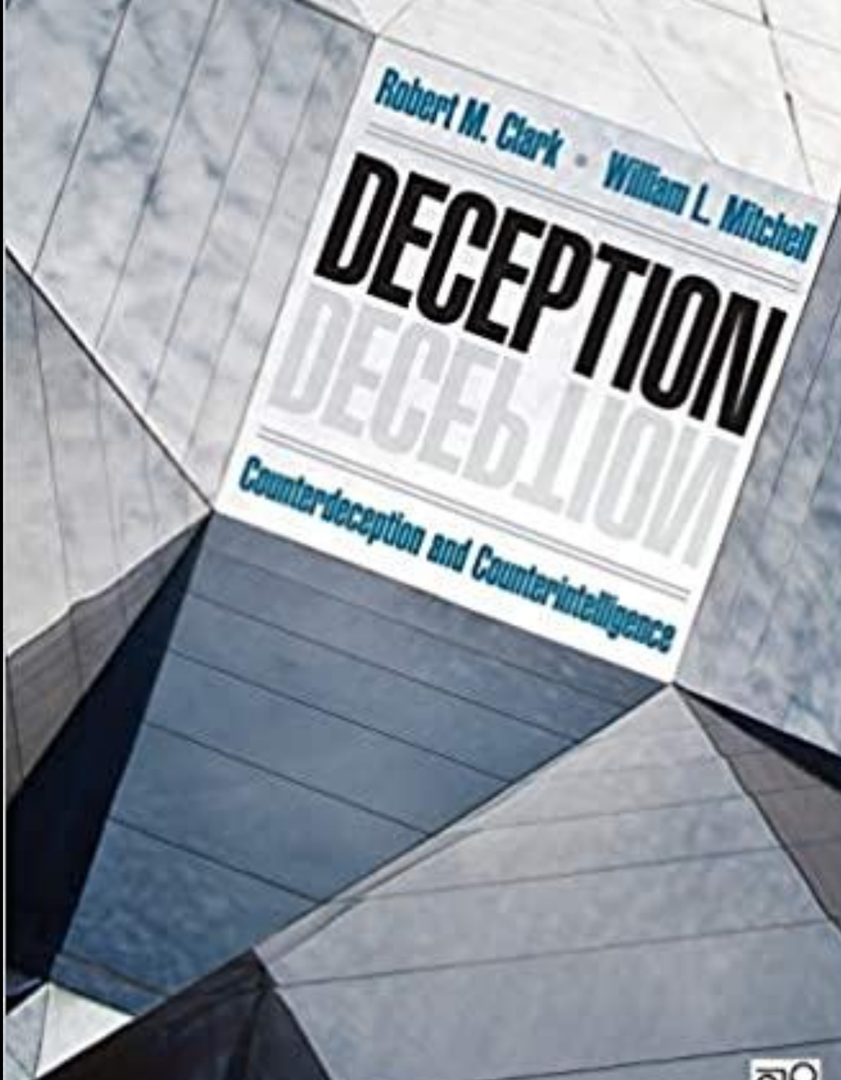
We can boil this down to **Deception** being:

- **Hiding the real**
- **Showing the fake**

“Deception is a process intended to advantageously impose the fake on a target’s perception of reality.”

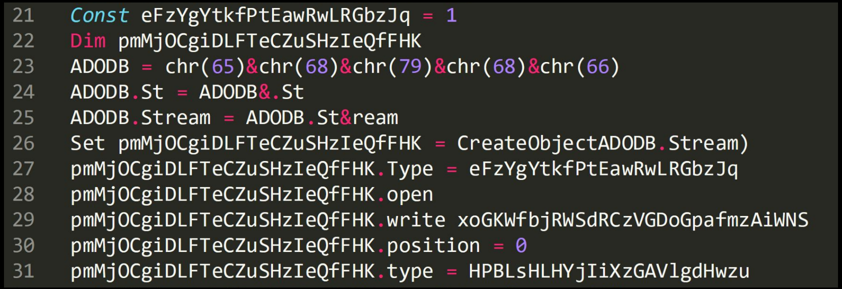
“One does not conduct deception for the sake of deception itself. It supports some overarching plan or objectives of a participant”

Robert M. Clark and
Dr. William L. Mitchell


Robert M. Clark • William L. Mitchell
DECEPTION
Counterdeception and Counterintelligence

- Hiding the real

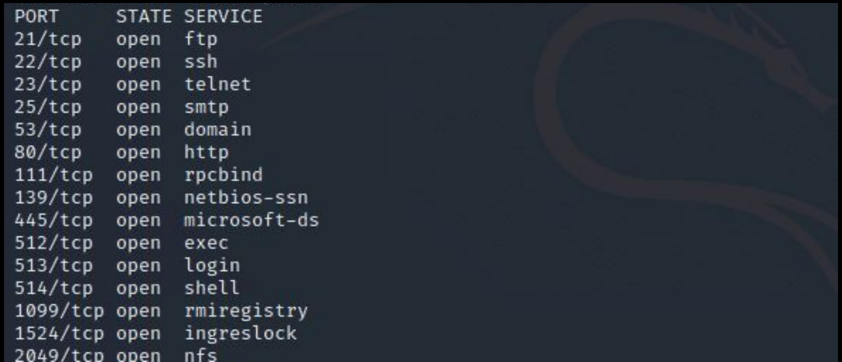
  Malware obfuscation



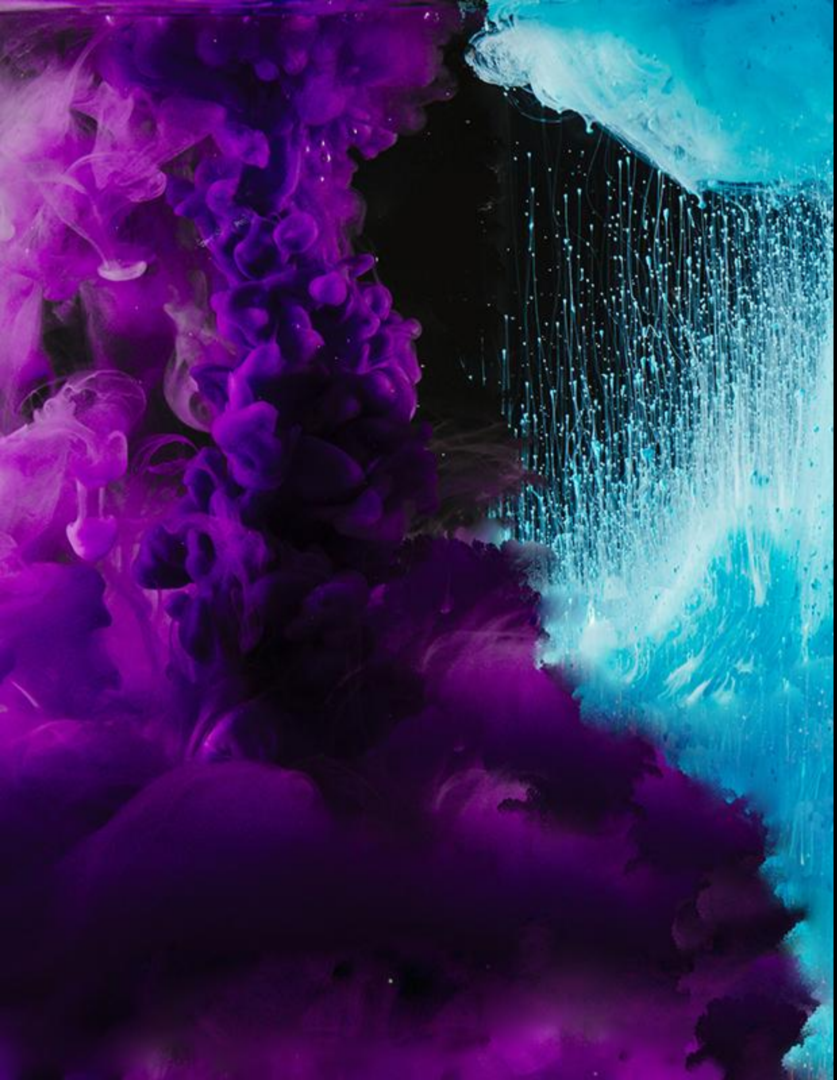
```
Const eFzYgYtkfPtEawRwLRGbzJq = 1
Dim pmMjOCgiDLFTeCZuSHzIeQfFHK
ADODB = chr(65)&chr(68)&chr(79)&chr(68)&chr(66)
ADODB.St = ADODB&.St
ADODB.Stream = ADODB.St&ream
Set pmMjOCgiDLFTeCZuSHzIeQfFHK = CreateObjectADODB.Stream)
pmMjOCgiDLFTeCZuSHzIeQfFHK.Type = eFzYgYtkfPtEawRwLRGbzJq
pmMjOCgiDLFTeCZuSHzIeQfFHK.open
pmMjOCgiDLFTeCZuSHzIeQfFHK.write xoGKWfbjRWSdRCzVGDoGpafmzAiWNS
pmMjOCgiDLFTeCZuSHzIeQfFHK.position = 0
pmMjOCgiDLFTeCZuSHzIeQfFHK.type = HPBLsHLHYjIiXzGAVlgdHwzu
```

- Showing the fake

  Artillery / all ports open



```
PORT      STATE SERVICE
21/tcp    open  ftp
22/tcp    open  ssh
23/tcp    open  telnet
25/tcp    open  smtp
53/tcp    open  domain
80/tcp    open  http
111/tcp   open  rpcbind
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
512/tcp   open  exec
513/tcp   open  login
514/tcp   open  shell
1099/tcp open  rmiregistry
1524/tcp open  ingreslock
2049/tcp open  nfs
```



From the CIA Do’s and Don’ts in regards to **hiding the real**:

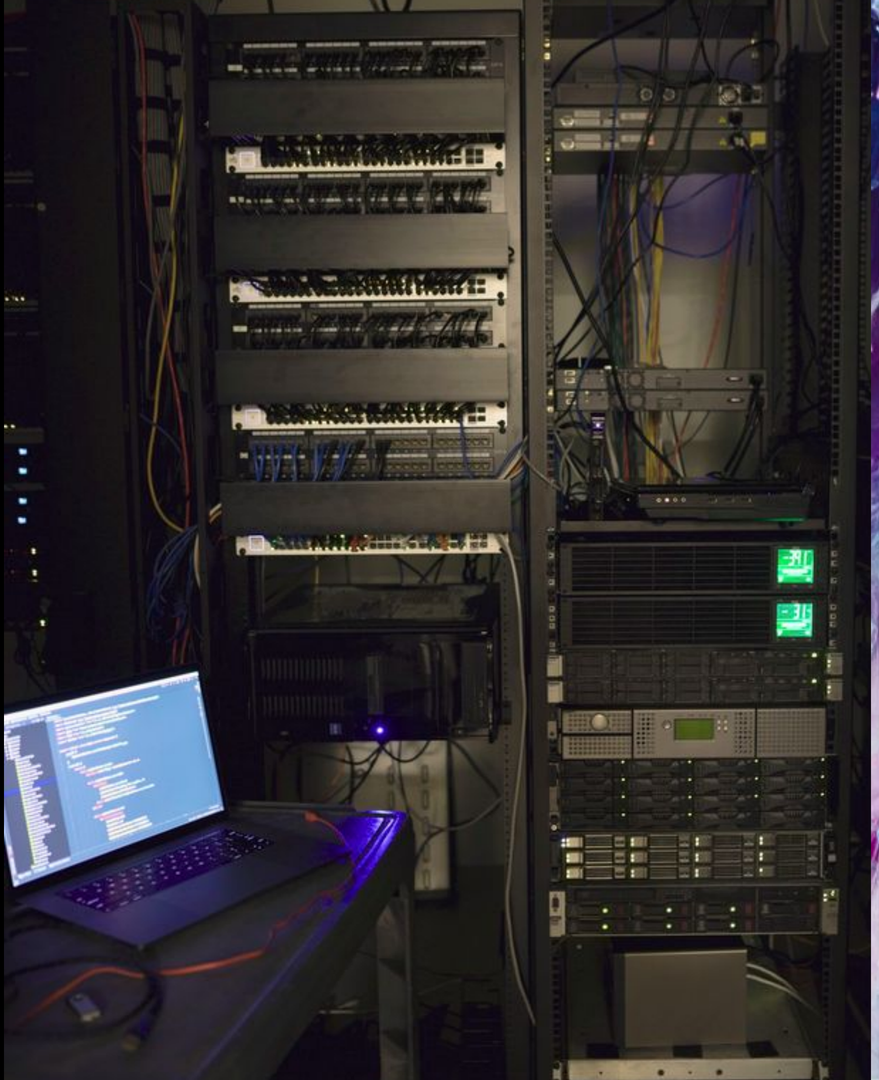
- DO obfuscate or encrypt all strings and configuration data that directly relate to tool functionality

- DO NOT decrypt or de-obfuscate all string data or configuration data immediately upon execution.

- DO strip all debug symbol information, manifests, build paths, developer usernames from the final build of a binary.

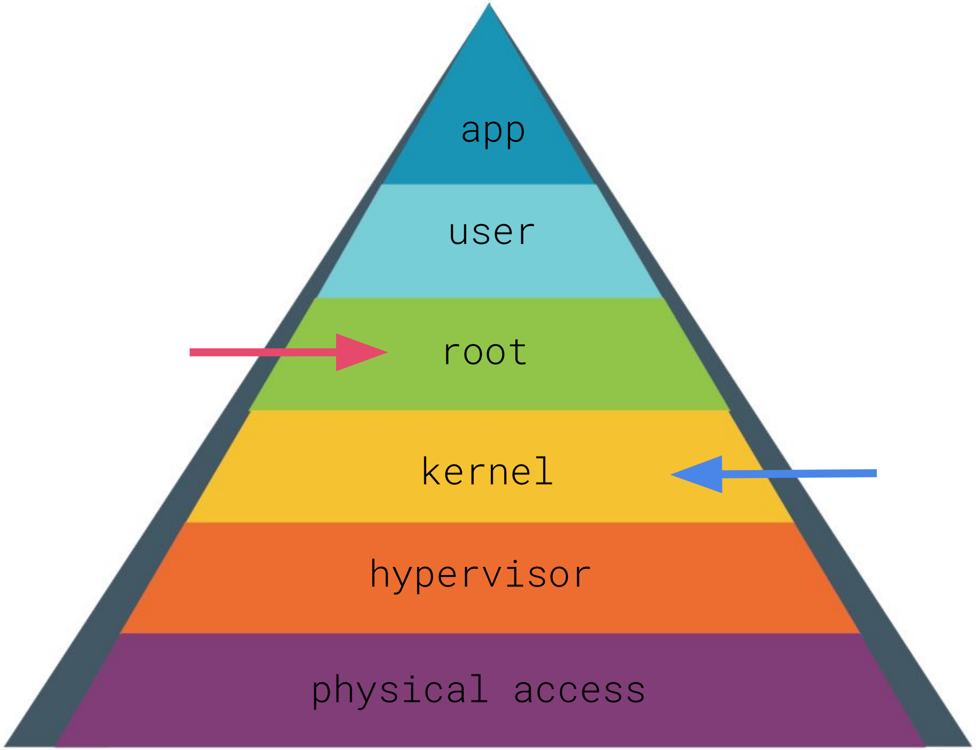
2. The Principle of Physical Access

States that physical control of a device grants a superior level of control, where the machine can be turned off, forensically analyzed, and reimaged.



Layers of control

The defense typically has physical control or a deeper level of control than the attacker, meaning they can cut network access, power off, perform dead disk forensics, and even reimage a machine.



Cryptography

Amazing tool, can protect confidentiality and integrity of data in hostile spaces

Cryptography doesn’t protect access, meaning the owner of the machine can always reformat or put new code / data there.

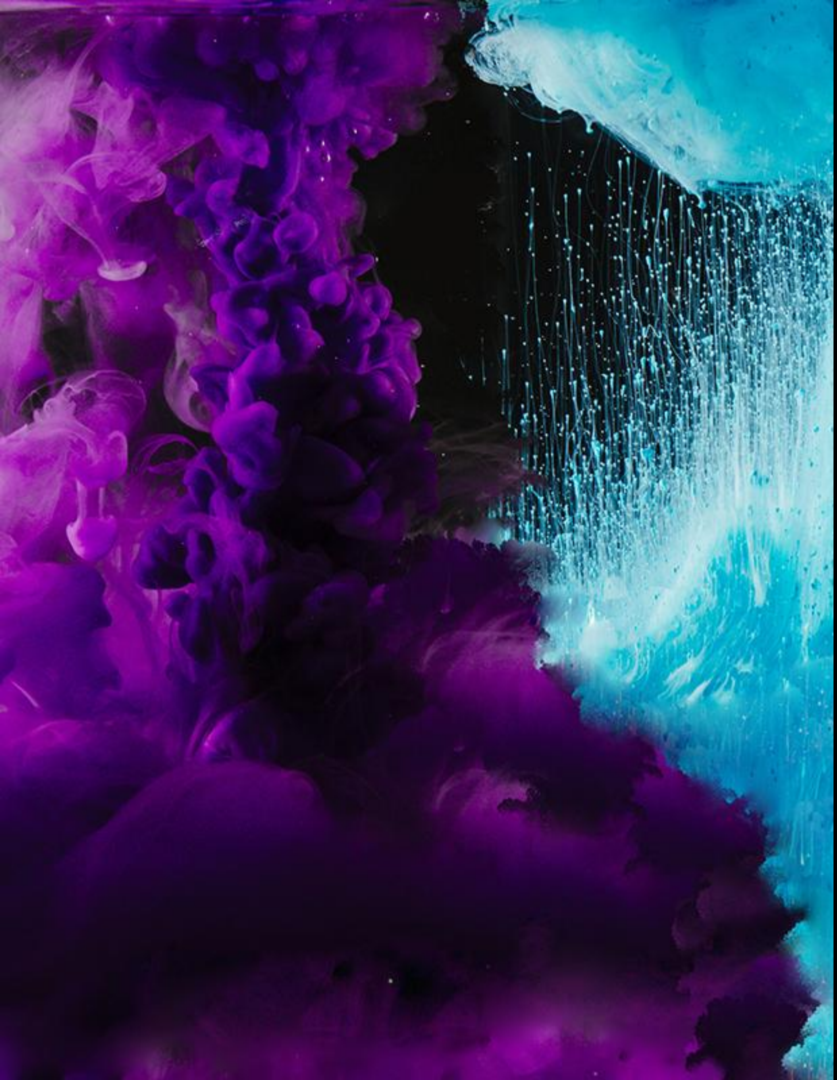
This means the offense can never overtly dominate the target network, as the owner with physical access can always regain access w/ time.

The offense’s natural path is through stealth if they want to persist for a long time.

Corollary here: Physical access often trumps digital access

Local and/or physical attacks are often more prevalent and impactful,

This means local and/or physical attacks are often a priority over digital security in a targeted situation or hostile enviorment

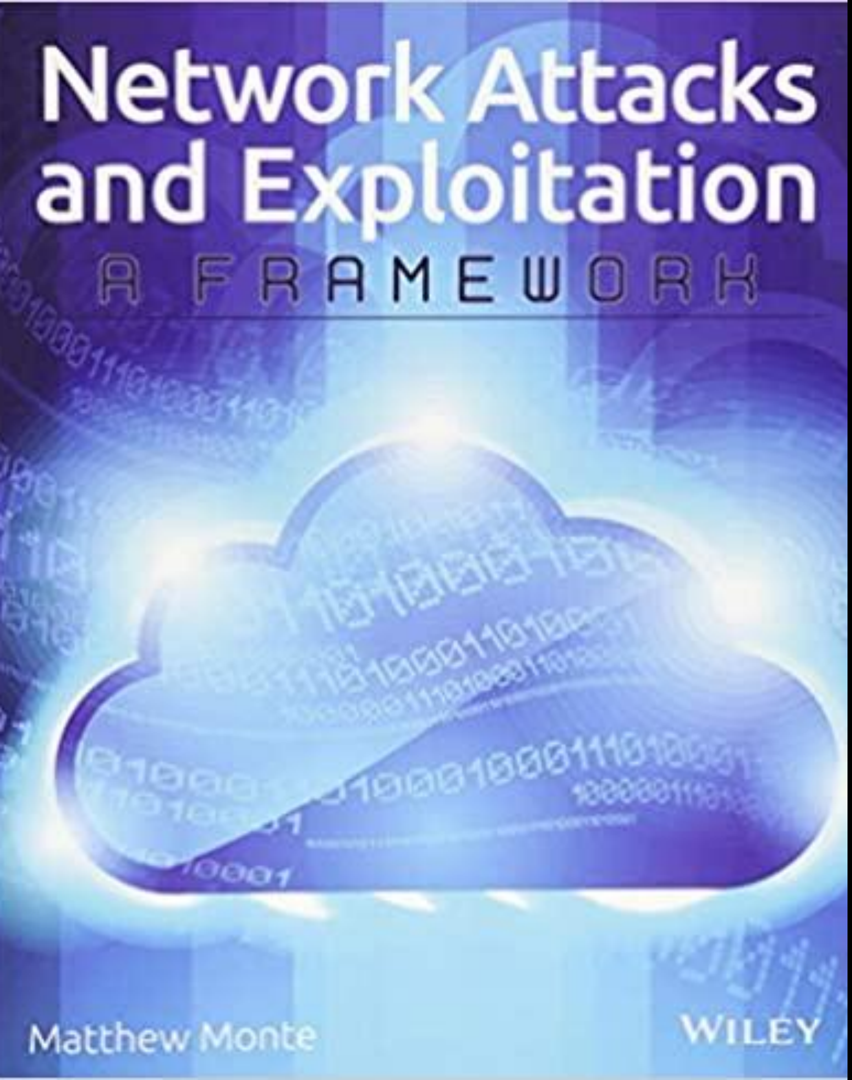


From the CIA Do’s and Don’ts in regards to **potential physical access**:

- DO encrypt all data written to disk.
- DO utilize a secure erase when removing a file from disk that wipes at a minimum the file’s filename, datetime stamps (create, modify and access) and its content.

3. Principle of Humanity

States that computers are fundamentally tools for humans, thus will have regular human users, interfaces for humans, and human mistakes.



This is two combined principles from Matthew Monette’s Book:
“Network Attacks and Exploitation: A Framework”

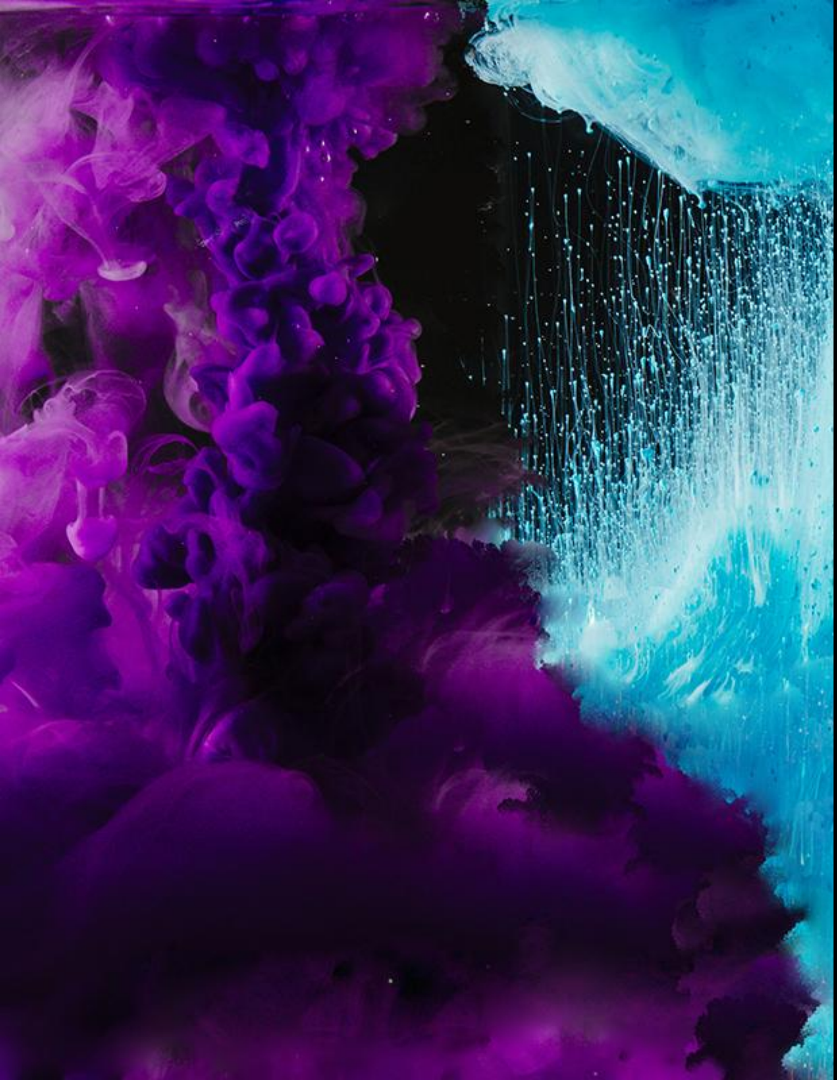
Principle of Access -
“Because data or systems must be accessed by humans there is always a viable path to their target data”

Principle of Humanity -
“CNE is grounded in human nature. The attacker [or defender] is a person or a group of people. [They] may be a lone actor, a well-ordered hierarchy, or a loose conglomeration of thousands, but regardless [they are] human”

What does this mean for us?

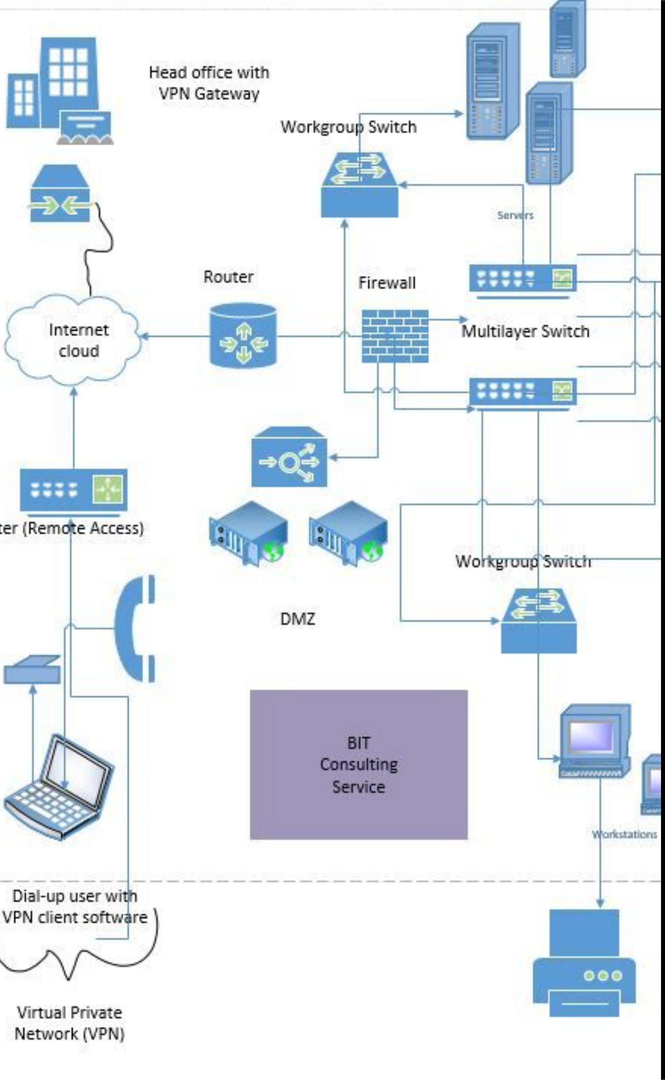
We can capitalize on human error. Computers are extremely complex. Software will be unpatched, operators will make mistakes.

We can target groups, operators, humans we are up against to better enable our own operations. Spear phishing for target access. Or attribution of a group for better detection.



From the CIA Do’s and Don’ts in regards to **manipulating the principle of humanity**:

- DO NOT perform operations that will cause the target computer to be unresponsive to the user (e.g. CPU spikes, screen flashes, screen “freezing”, etc).
- DO NOT have “dirty words” (see dirty word list – TBD) in the binary.

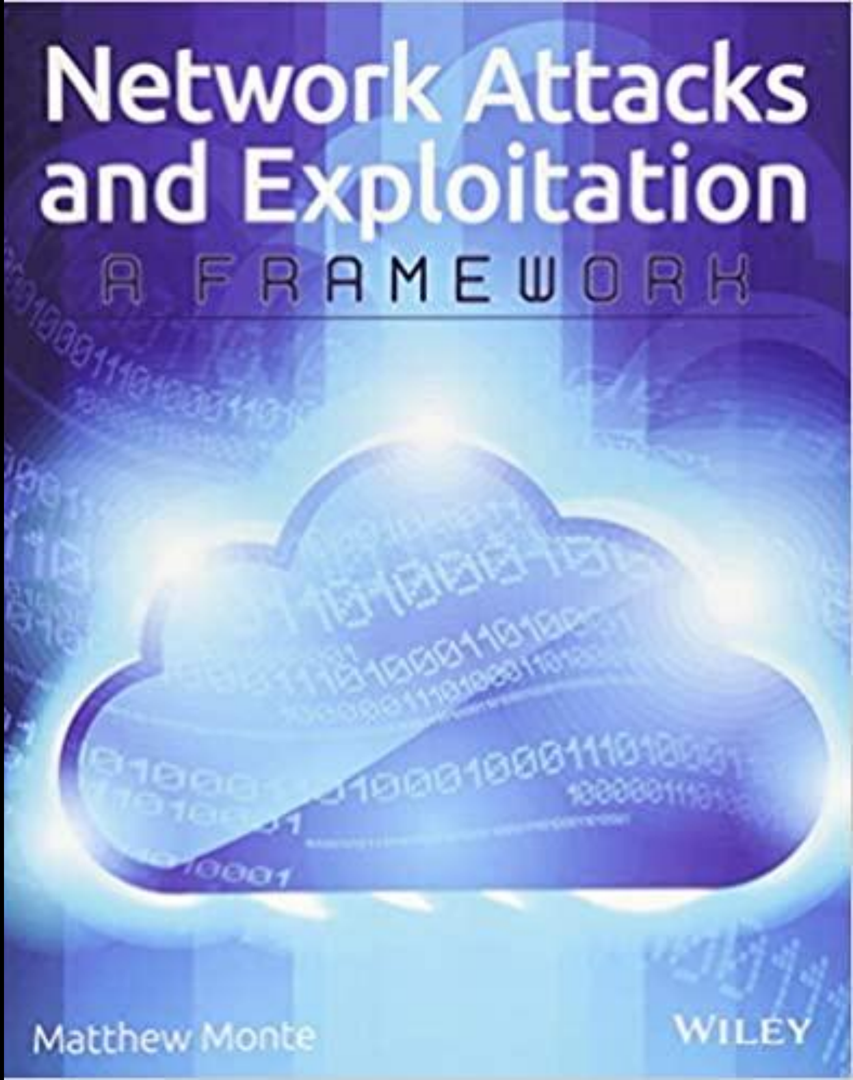


4. Principle of Economy

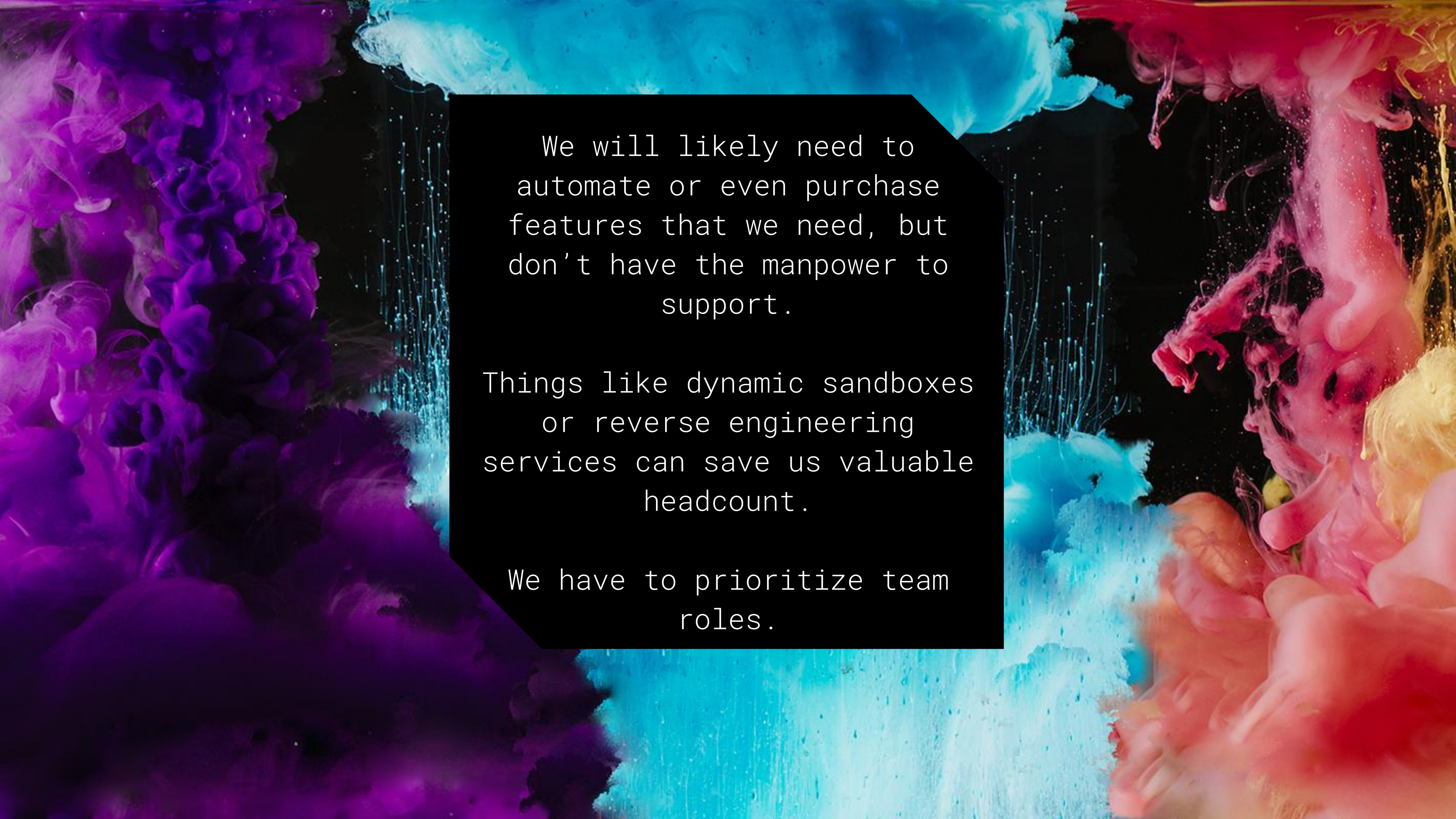
States that both offensive and defensive teams have limited budgets and can only invest in so many strategies or initiatives for their operations.

This principle also comes from Matthew Monette’s Book: “Network Attacks and Exploitation: A Framework”

> “Ambitions will always exceed available resources.”



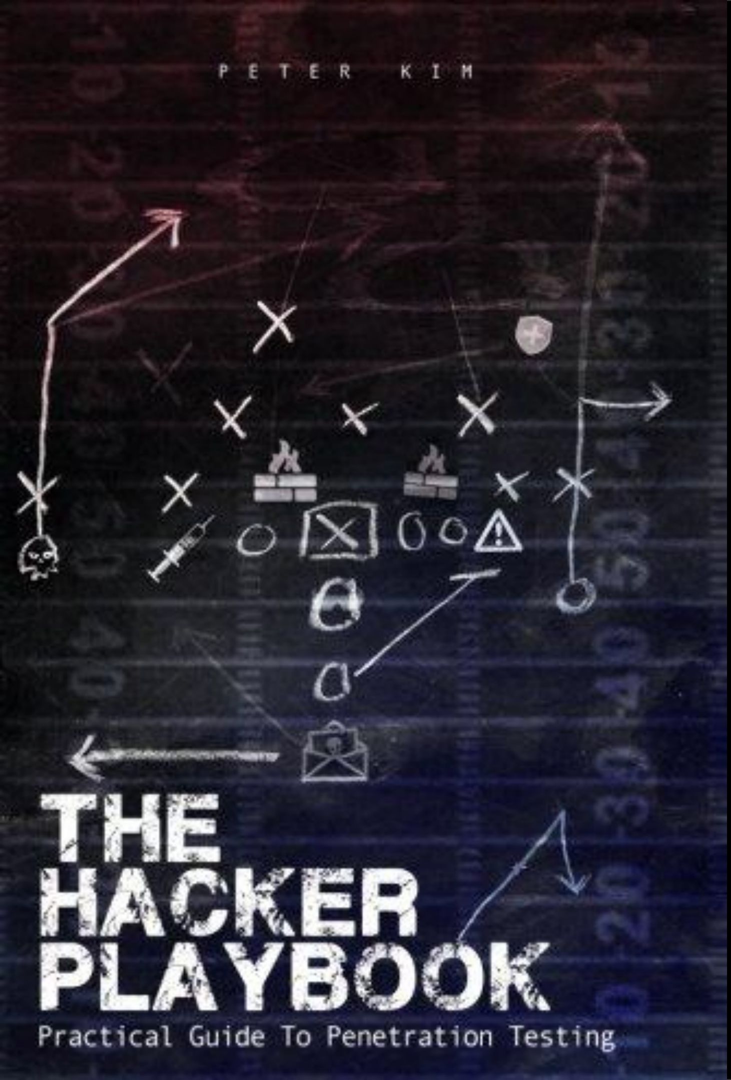
CCDC is often 3 (or 2) attackers against 8 defenders, which means we can't play "1-on-1" on the offense.



We will likely need to automate or even purchase features that we need, but don’t have the manpower to support.

Things like dynamic sandboxes or reverse engineering services can save us valuable headcount.

We have to prioritize team roles.



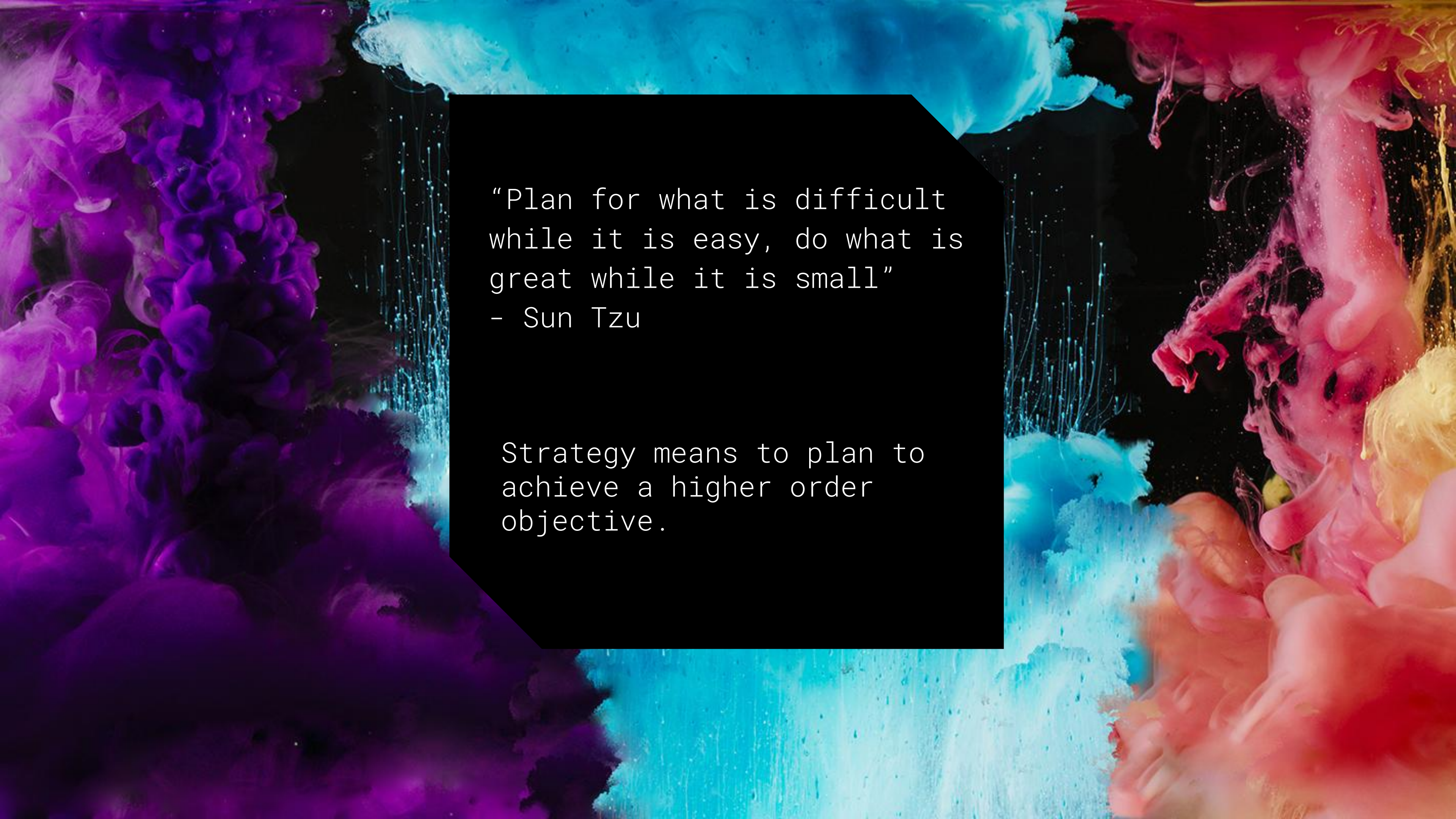
5. Principle of Planning

States that writing down or automating plans will provide an advantage when dealing with the complexity of computers in a high stress situation.

We can mitigate errors we will know will be there from the principle of humanity.

We can easily plan for repeatable and predictable engagements, like pentest engagement and report writing.

Creating a process and tools around the mundane standardizes it and produces higher quality work.

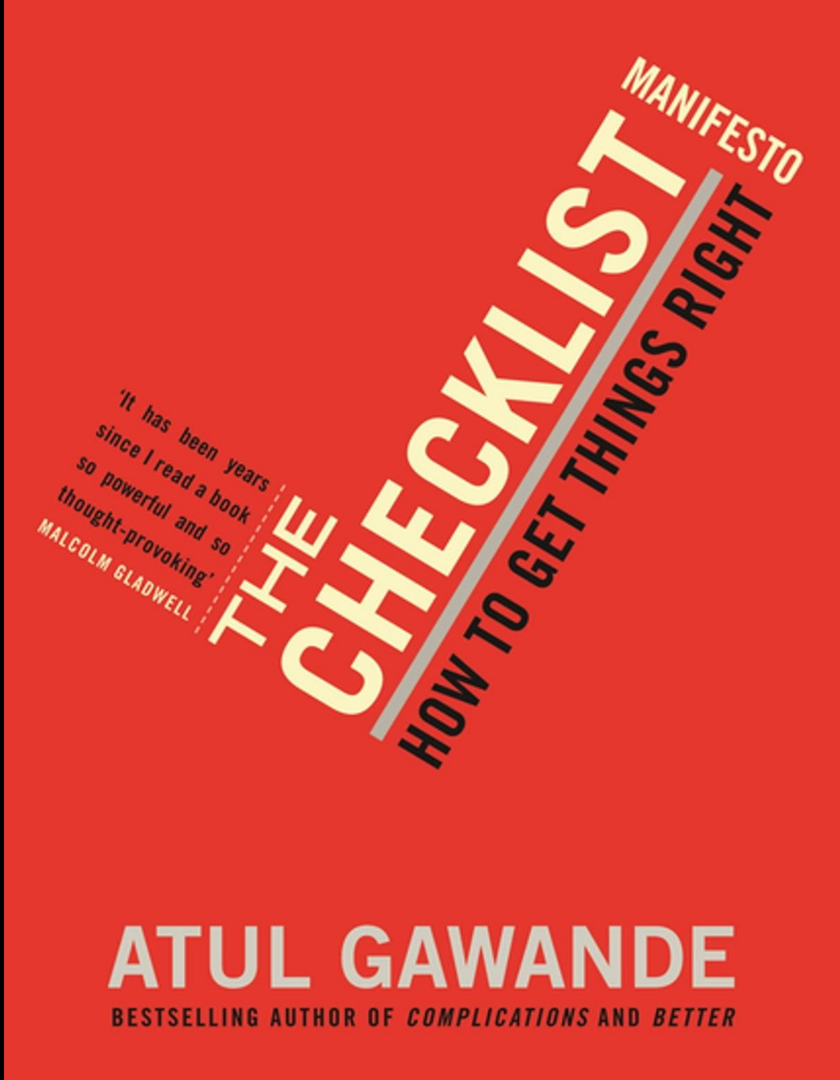


“Plan for what is difficult while it is easy, do what is great while it is small”
- Sun Tzu

Strategy means to plan to achieve a higher order objective.

Flight checklists made the model 299 (B-17 Flying Fortress) flyable, changing the history of WWII and flight all together.

Checklist Manifesto

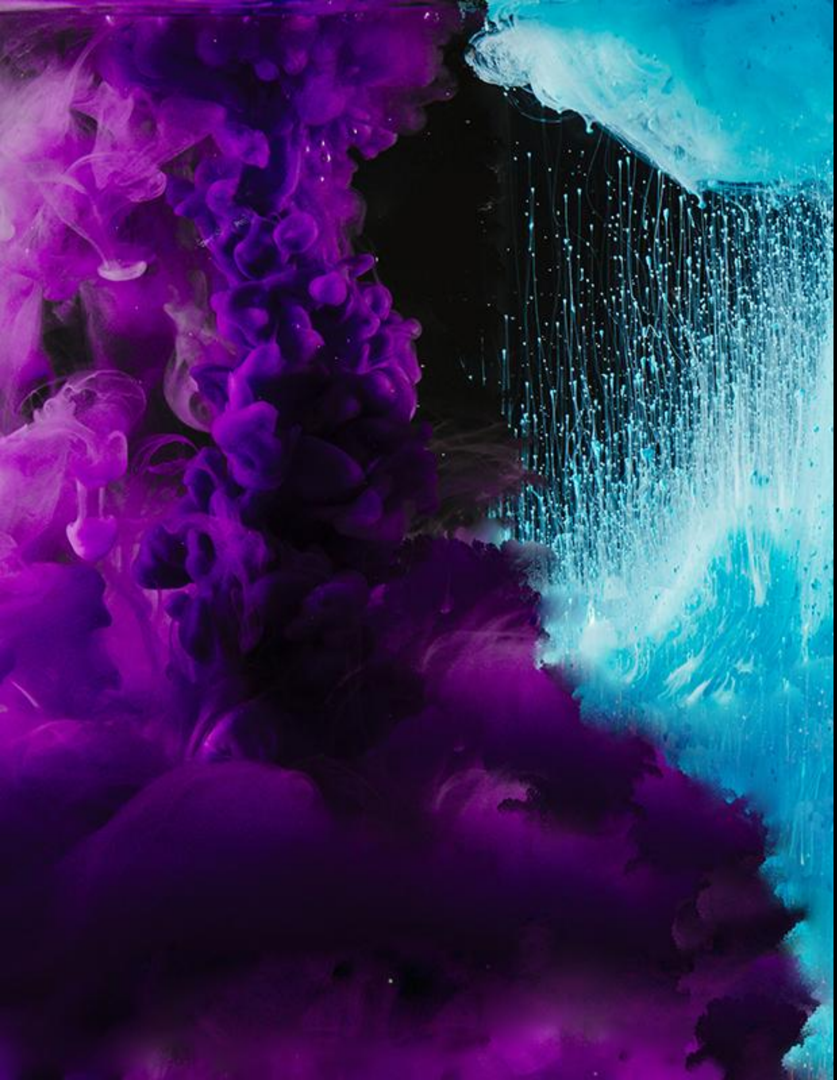

'It has been years since I read a book so powerful and so thought-provoking'
MALCOLM GLADWELL
THE CHECKLIST MANIFESTO
HOW TO GET THINGS RIGHT
ATUL GAWANDE
BESTSELLING AUTHOR OF COMPLICATIONS AND BETTER

Planning in cyber security is critical. You may do it unconsciously, you may do it consciously, every org with an IR or DR/BC plan has done it. Same with preparing tools for a common pentest, threat modeling an org, or preparing detection systems is planning

In competitions we plan out the out the first 10 minute, the first hour, first half day, first day. and second day.

Having these mile stones where we know we have prior strategy makes it that much more effective.

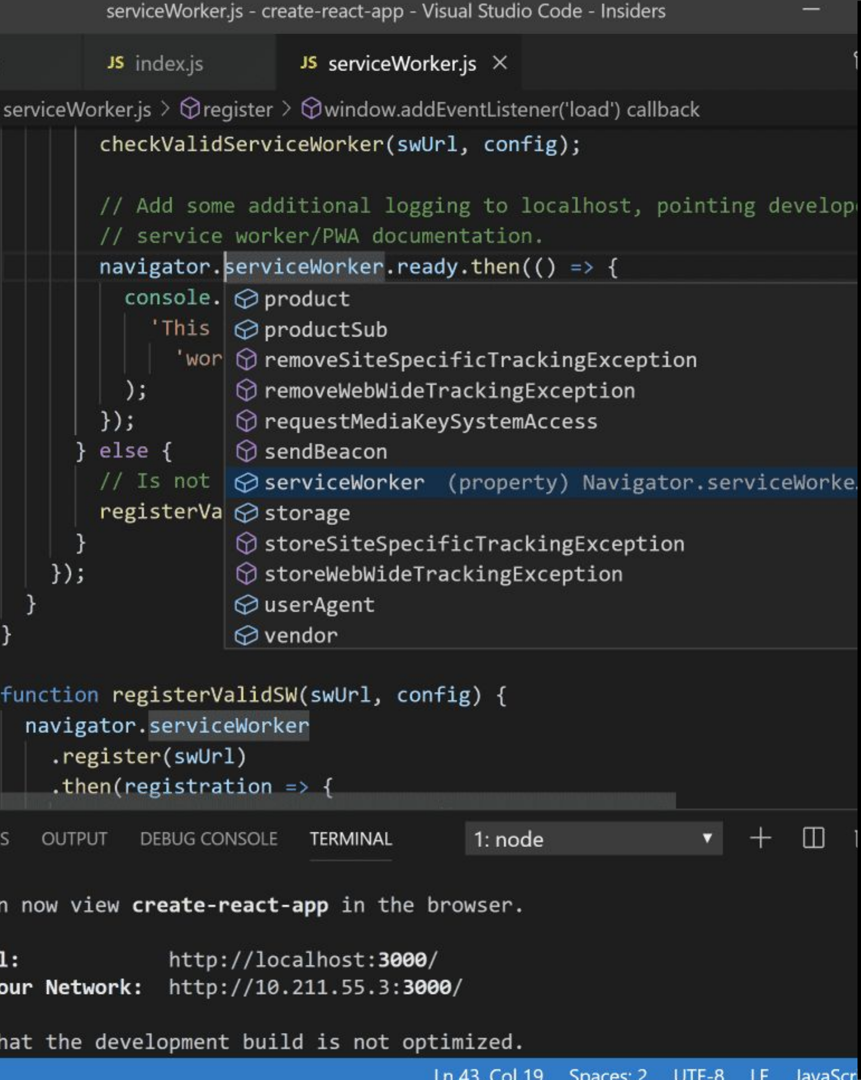
Contingency Planning -
When the plan goes wrong,
be ready to adapt



From the CIA Do’s and Don’ts in regards to **planning operations**:

- DO provide a means to completely “uninstall”/”remove” implants, function hooks, injected threads, dropped files, registry keys, services, forked processes, etc whenever possible. Explicitly document (even if the documentation is “There is no uninstall for this “) the procedures, permissions required and side effects of removal.

- DO explicitly document the “disk forensic footprint” that could be potentially created by various features of a binary/tool on a remote target.


serviceWorker.js - create-react-app - Visual Studio Code - Insiders
JS index.js
JS serviceWorker.js
serviceWorker.js > register > window.addEventListener('load') callback

```
      checkValidServiceWorker(swUrl, config);

      // Add some additional logging to localhost, pointing develop
      // service worker/PWA documentation.
      navigator.serviceWorker.ready.then(() => {
        console.
          'This
            'wor
        );
      });
    } else {
      // Is not
      registerVa
    }
  });
 }
}

function registerValidSW(swUrl, config) {
  navigator.serviceWorker
    .register(swUrl)
    .then(registration => {
```

product
productSub
removeSiteSpecificTrackingException
removeWebWideTrackingException
requestMediaKeySystemAccess
sendBeacon
serviceWorker (property) Navigator.serviceWorke
storage
storeSiteSpecificTrackingException
storeWebWideTrackingException
userAgent
vendor
S OUTPUT DEBUG CONSOLE TERMINAL
1: node

```
n now view create-react-app in the browser.

l:            http://localhost:3000/
our Network:  http://10.211.55.3:3000/

hat the development build is not optimized.
```

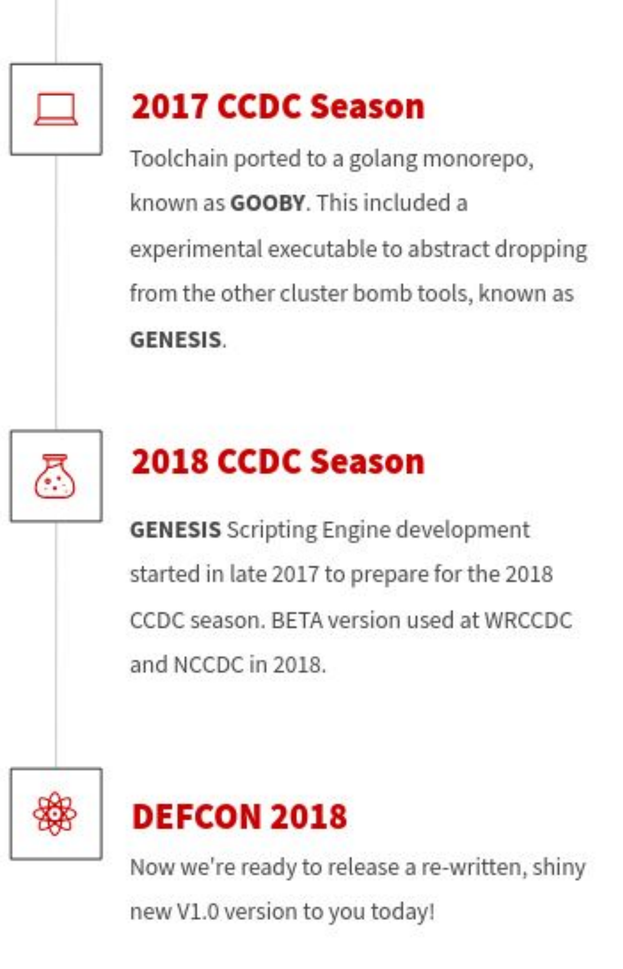
6. Principle of Innovation

States that the high level of complexity in computing makes it easy to innovate as well as providing noticeable advantages in a competition environment.

What is innovation?

Innovation can be any change that makes,simplifies, combines, provides new capabilities, or even exploits a feature

It can change the tempo of conflict, innovation can help subvert expectations or assumptions the opponent has made.



2017 CCDC Season

Toolchain ported to a golang monorepo, known as **GOOBY**. This included a experimental executable to abstract dropping from the other cluster bomb tools, known as **GENESIS**.

2018 CCDC Season

GENESIS Scripting Engine development started in late 2017 to prepare for the 2018 CCDC season. BETA version used at WRCCDC and NCCDC in 2018.

DEFCON 2018

Now we're ready to release a re-written, shiny new V1.0 version to you today!

New tool dev is super easy in computer security

We can automate our previous plans with technology to make them seamless and automatic.

We can continue to innovate on old concepts, making them faster, simpler, and with more features.

We get value out of finding new ways to accomplish objectives, such as an attacker avoiding detection of old tool signatures

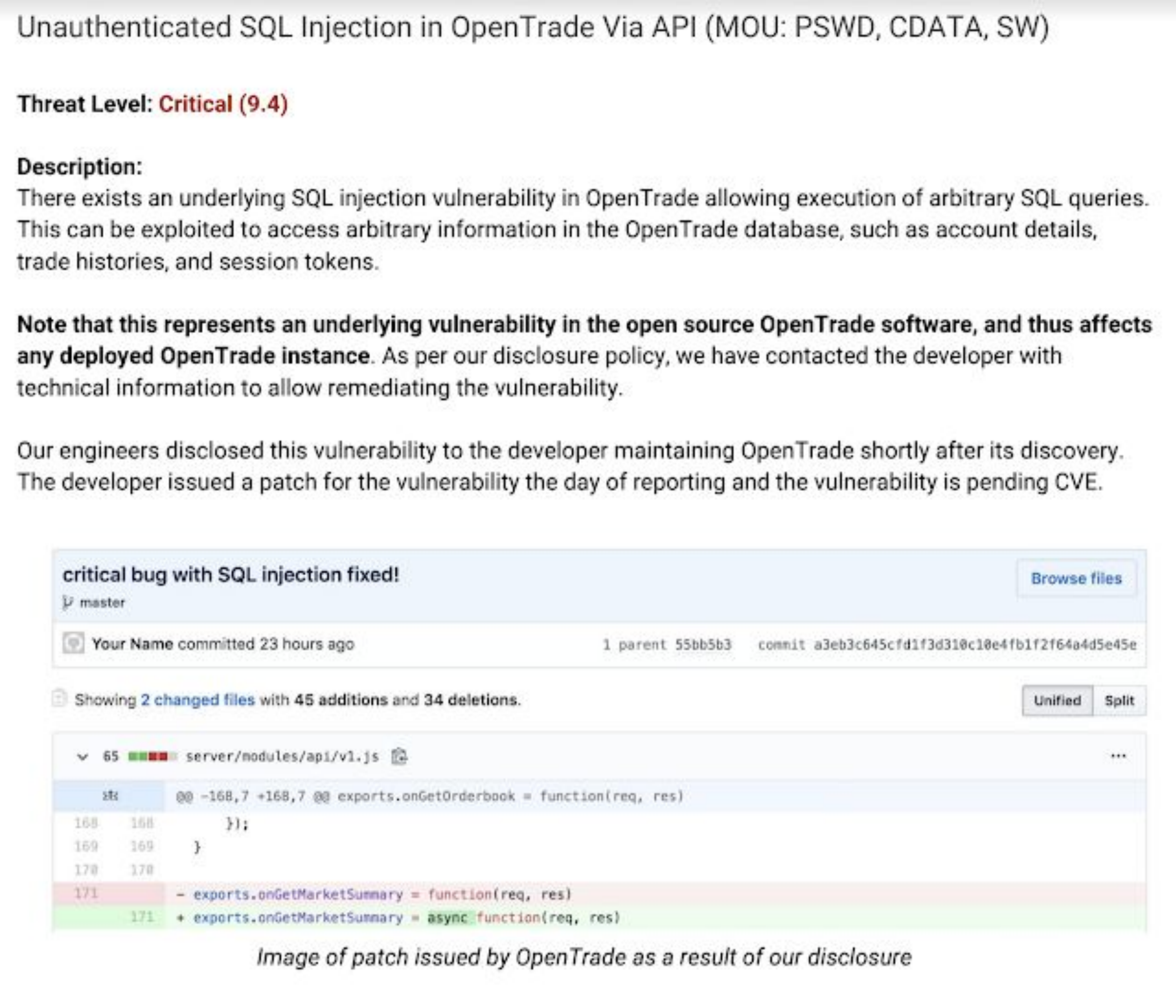
Like deception, we shouldn’t innovate just for the sake of innovation, it should be to support something.

“Necessity is the mother of all invention” - it is more important to innovate the right thing to have a deeper impact

0 day dev

Forging new access through innovation

CPTC has now seen multiple 0day vulnerabilities reported between our regional and final events in subsequent years



Unauthenticated SQL Injection in OpenTrade Via API (MOU: PSWD, CDATA, SW)

Threat Level: Critical (9.4)

Description:
There exists an underlying SQL injection vulnerability in OpenTrade allowing execution of arbitrary SQL queries. This can be exploited to access arbitrary information in the OpenTrade database, such as account details, trade histories, and session tokens.

Note that this represents an underlying vulnerability in the open source OpenTrade software, and thus affects any deployed OpenTrade instance. As per our disclosure policy, we have contacted the developer with technical information to allow remediating the vulnerability.

Our engineers disclosed this vulnerability to the developer maintaining OpenTrade shortly after its discovery. The developer issued a patch for the vulnerability the day of reporting and the vulnerability is pending CVE.

critical bug with SQL injection fixed!

Your Name committed 23 hours ago   1 parent 55bb5b3   commit a3eb3c645cfd1f3d310c10e4fb1f2f64a4d5e45e

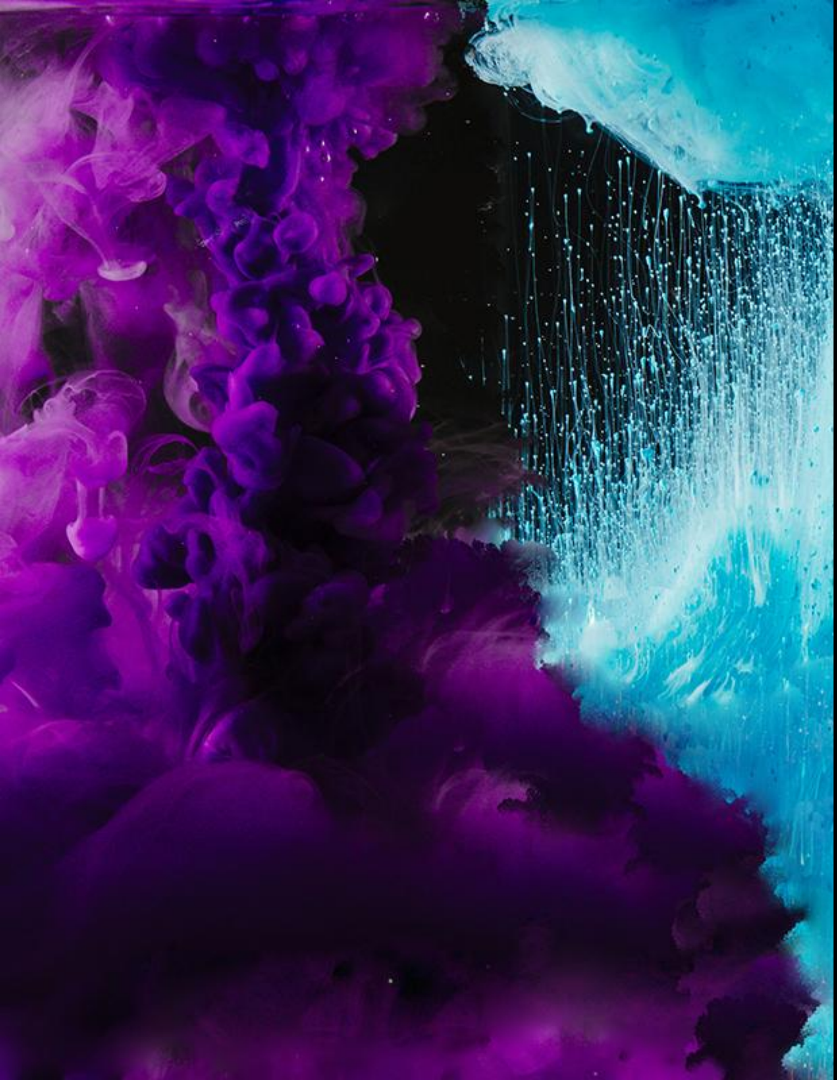
Showing 2 changed files with 45 additions and 34 deletions.

65 server/modules/api/v1.js

```
@@ -168,7 +168,7 @@ exports.onGetOrderbook = function(req, res)
         });
   }

- exports.onGetMarketSummary = function(req, res)
+ exports.onGetMarketSummary = async function(req, res)
```

Image of patch issued by OpenTrade as a result of our disclosure



From the CIA Do’s and Don’ts in regards to **new tool dev**:

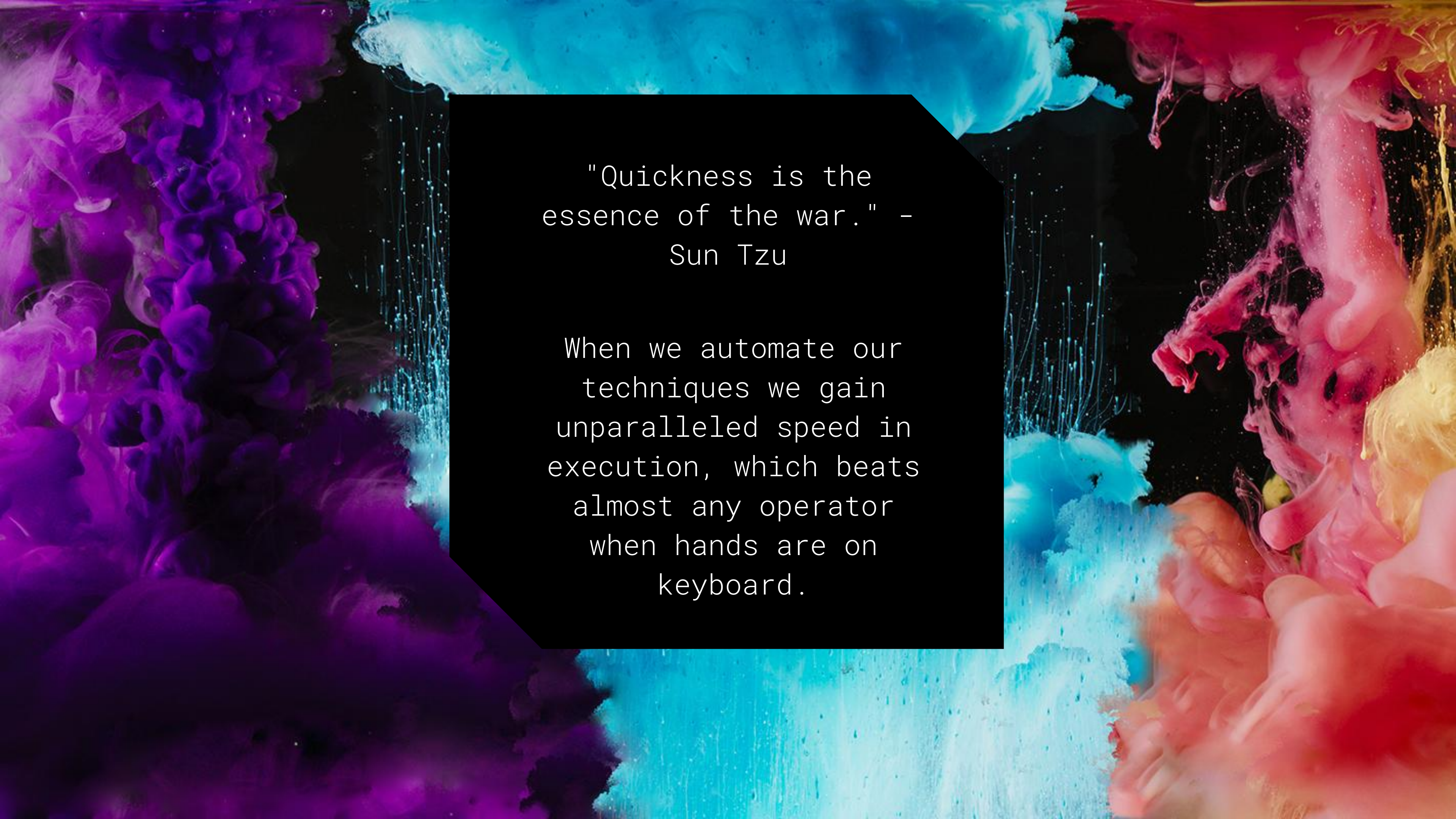
- DO use end-to-end encryption for all network communications. NEVER use networking protocols which break the end-to-end principle with respect to encryption of payloads.
- DO NOT allow network traffic, such as C2 packets, to be re-playable.
- DO NOT use hard-coded filenames or filepaths when writing files to disk.

7. Principle of Time

States that timing is critical in regards to computer conflict. There are many ways to take advantage of timing, such as automation and bit rot.

Timing of attacks

Timing +
Deception =
Surprise

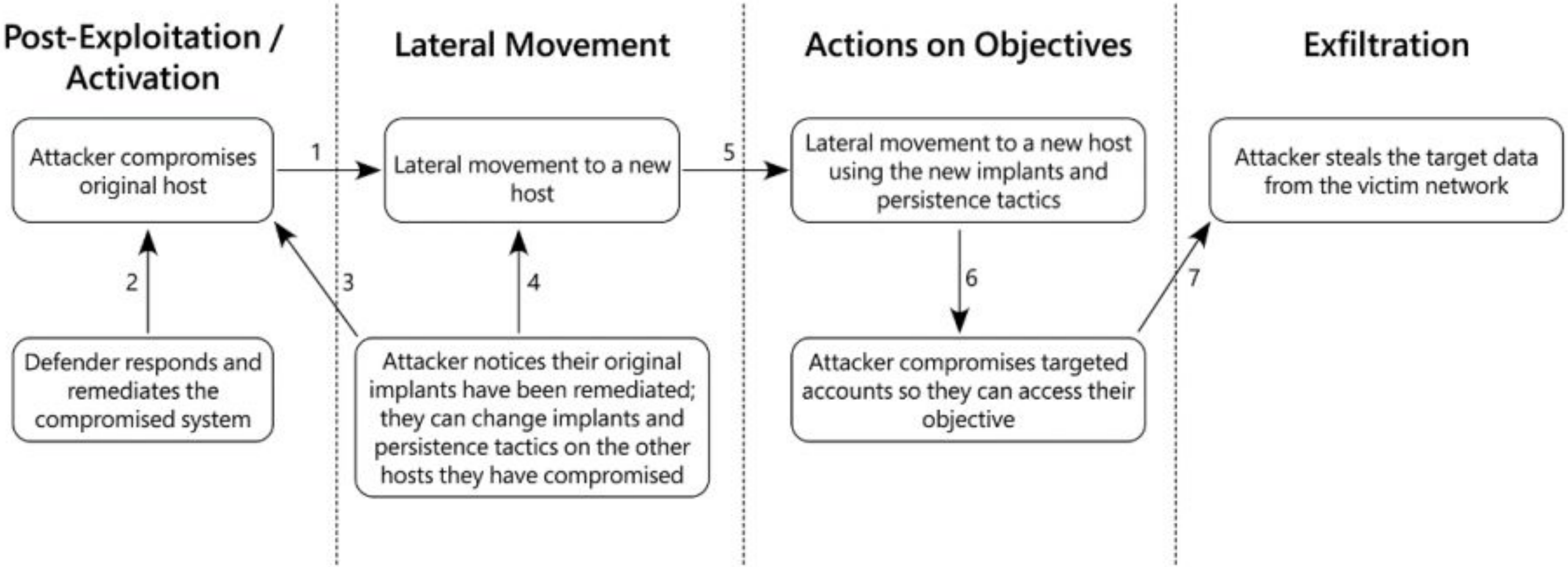


"Quickness is the essence of the war." - Sun Tzu

When we automate our techniques we gain unparalleled speed in execution, which beats almost any operator when hands are on keyboard.

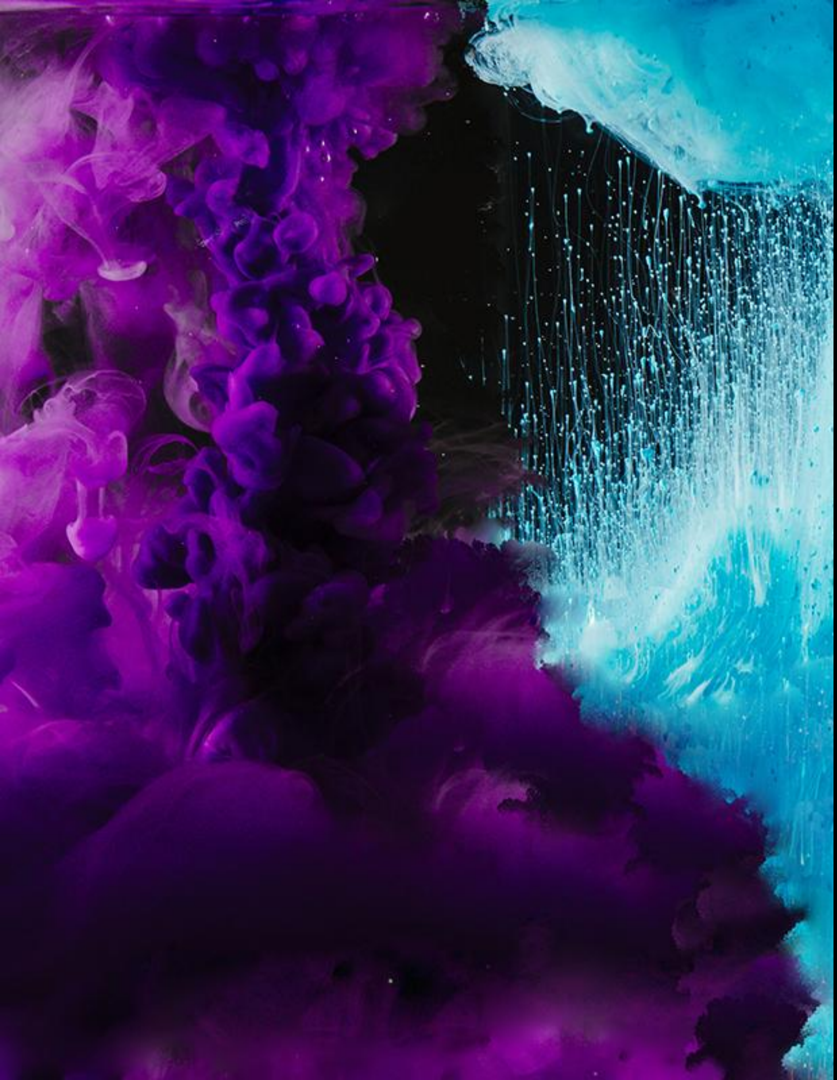
Timeline the attack as a defender

Defender’s Fallacy - Responding too soon


Post-Exploitation / Activation
Lateral Movement
Actions on Objectives
Exfiltration
Attacker compromises original host
1
Lateral movement to a new host
5
Lateral movement to a new host using the new implants and persistence tactics
Attacker steals the target data from the victim network
2
3
4
6
7
Defender responds and remediates the compromised system
Attacker notices their original implants have been remediated; they can change implants and persistence tactics on the other hosts they have compromised
Attacker compromises targeted accounts so they can access their objective

Bitrot

Systems inherently become weaker over time as new vulns are found



From the CIA Do’s and Don’ts in regards to **temporal based operations**:

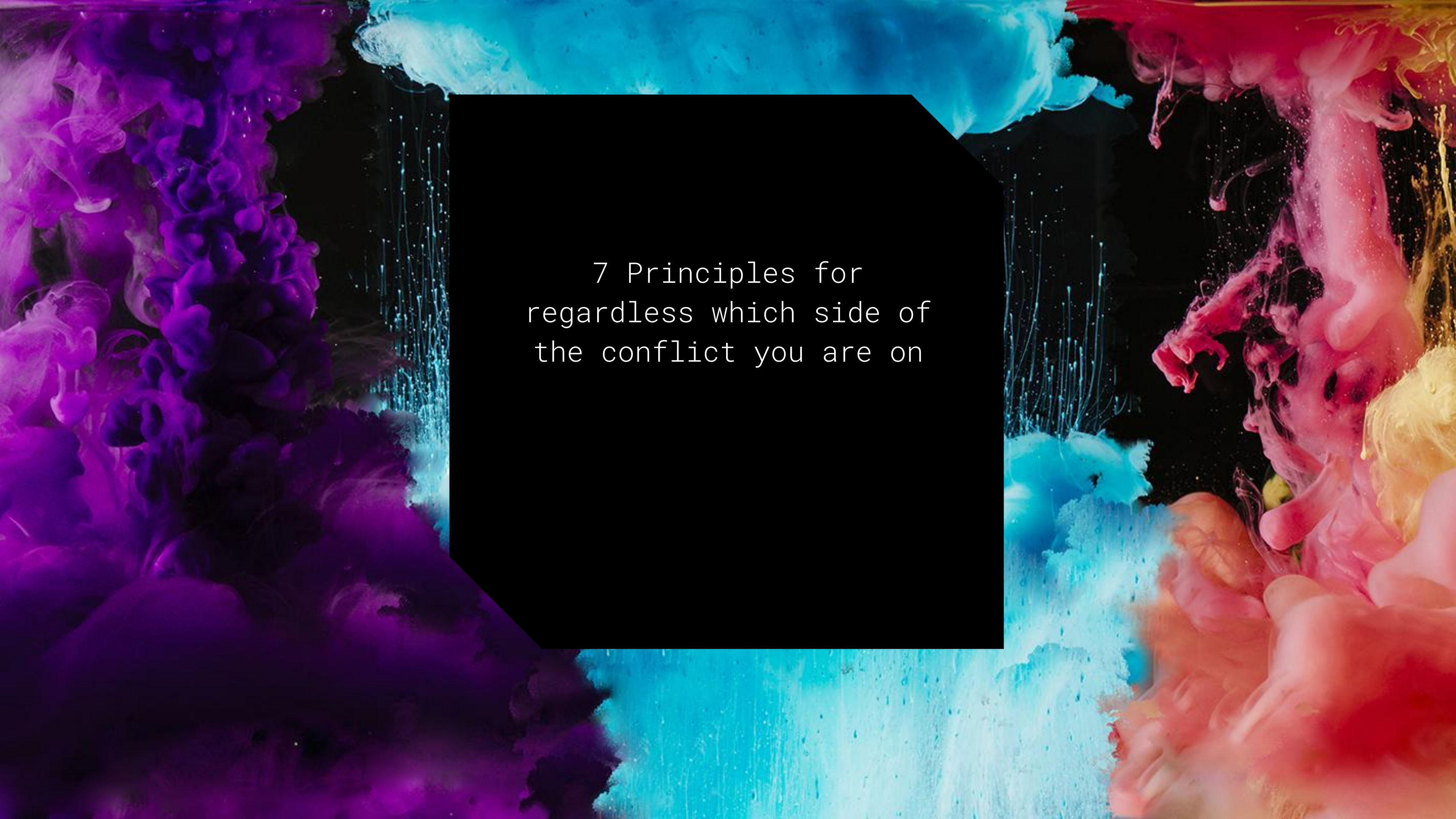
- DO explicitly remove sensitive data from memory as soon as the data is no longer needed in plain-text form.

- DO utilize a deployment-time unique key for obfuscation/de-obfuscation of sensitive strings and configuration data.

- DO use variable size and timing (aka jitter) of beacons/network communications. DO NOT predicatively send packets with a fixed size and timing.

- DO use GMT/UTC/Zulu as the time zone when comparing date/time.

Take Aways



7 Principles for regardless which side of the conflict you are on

The Principles are

1. Principle of **Deception**
    1.1. The use of deception, will help us get an advantage over an opponent in a computer conflict.

2. Principle of **Physical Access**
    2.1. Physical access of a device grants a superior level of control.

3. Principle of **Humanity**
    3.1. Computers are fundamentally tools for humans.

4. Principle of **Economy**
    4.1. Both offensive and defensive teams have limited budgets.

5. Principle of **Planning**
    5.1. Writing down or automating plans will provide an advantage.

6. Principle of **Innovation**
    6.1. The high level of complexity in computing makes it easier to innovate.

7. Principle of **Time**
    7.1. Timing is critical in regards to computer conflict.

8.

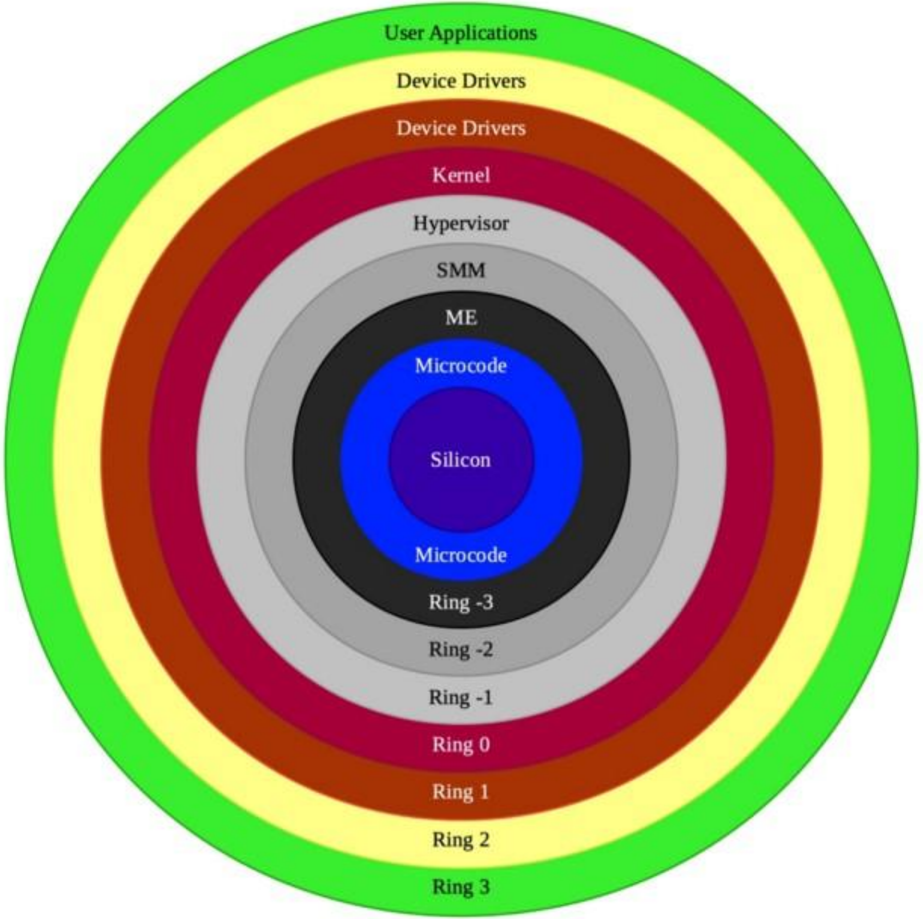
Q&A

Extras:

Twitter: https://twitter.com/1njection

Book: https://ahhh.github.io/Cybersecurity-Tradecraft/

Jobs: https://scale.com/careers/4061291005



User Applications

Device Drivers

Device Drivers

Kernel

Hypervisor

SMM

ME

Microcode

Silicon

Microcode

Ring -3

Ring -2

Ring -1

Ring 0

Ring 1

Ring 2

Ring 3

IA Hardware View

These are some simplified summaries:

1. Principle of **Deception**
    - States that the use of deception, will help us get an advantage over an opponent in a computer conflict.
2. Principle of **Physical Access**
    - States that physical control of a device grants a superior level of control.
3. Principle of **Humanity**
    - States that computers are fundamentally tools for humans.
4. Principle of **Economy**
    - States that both offensive and defensive teams have limited budgets.
5. Principle of **Planning**
    - States that writing down or automating plans will provide an advantage.
6. Principle of **Innovation**
    - States that the high level of complexity in computing makes it easier to innovate.
7. Principle of **Time**
    - States that timing is critical in regards to computer conflict.