



OWASP

Open Web Application  
Security Project

# “A holistic view on Cyber Security in evolutionary terms” (food-for-thought)

Dr. Grigorios Fragkos

Information Security Professional – EY OTS/TAS Cyber Security



@drgfragkos

# Agenda

*“our **security** mindset”*

*“intended to spark a personal **eureka** moment in the **mindmap** of each security professional inside and outside this room”*

# The Red Queen hypothesis

*“ The **Red Queen hypothesis**, also referred to as the Red Queen effect, is an evolutionary hypothesis which proposes that organisms must constantly **adapt**, **evolve**, and **proliferate**, not merely to gain a reproductive advantage, but also simply to survive while pitted against ever-evolving rival organisms in a continuously changing environment ”*

[goo.gl/rrzVvi](http://goo.gl/rrzVvi)



# The Threat Landscape

*“Now here, you see, it takes all the running  
you can do, to keep in the same place”*



# The Cyber Security in evolutionary terms

*“As **cyber threats** evolve, we need to be in a position to equally evolve, otherwise we simply keep **“running”** just to stay at the same place ”*





# Lets discuss...



*“ What is **Security** ? ”*

*“ What is **Cyber** ? ”*

*“ What is **Cyber Security** ? ”*

# What is Security?

*The Cambridge Dictionary describes **security** as:*

***“The ability to avoid being harmed by any risk, danger or threat”***

*The Oxford English Dictionary describes **security** as:*

***“The state of being or feeling secure”***

*...where “secure” is described as “protected against attack or other criminal activity”*



# What is Security?

*The ISO 28001 describes **security** as:*

***“resistance to intentional acts designed to cause harm or damage to or by the supply chain”***

*The ISO 17522 describes **security** as:*

***“combination of confidentiality, integrity, and availability”***

# What is Security?

*The ISO 20000 describes **information security** as:  
“preservation of confidentiality, integrity and availability of information”*

*The Wikipedia page describes **security** as:  
“Security resilience against, potential harm (or other unwanted coercive change) from external forces”*

# What is Cybersecurity?

The ISO 27032 describes **cybersecurity** as:

***“preservation of confidentiality, integrity and availability of information in the Cyberspace”***

The ISO 17522 describes **security** as:

***“combination of confidentiality, integrity, and availability”***

*...where “secure” is described as “protected against attack or other criminal activity”*

# Security in the context of the Information Age

*“The state of being or feeling **secure**, by having the ability to avoid being harmed **at an irrecoverable level**, by any risk, danger or threat, when/for protecting a specific asset”*

# The **Security** of Digital Ecosystems

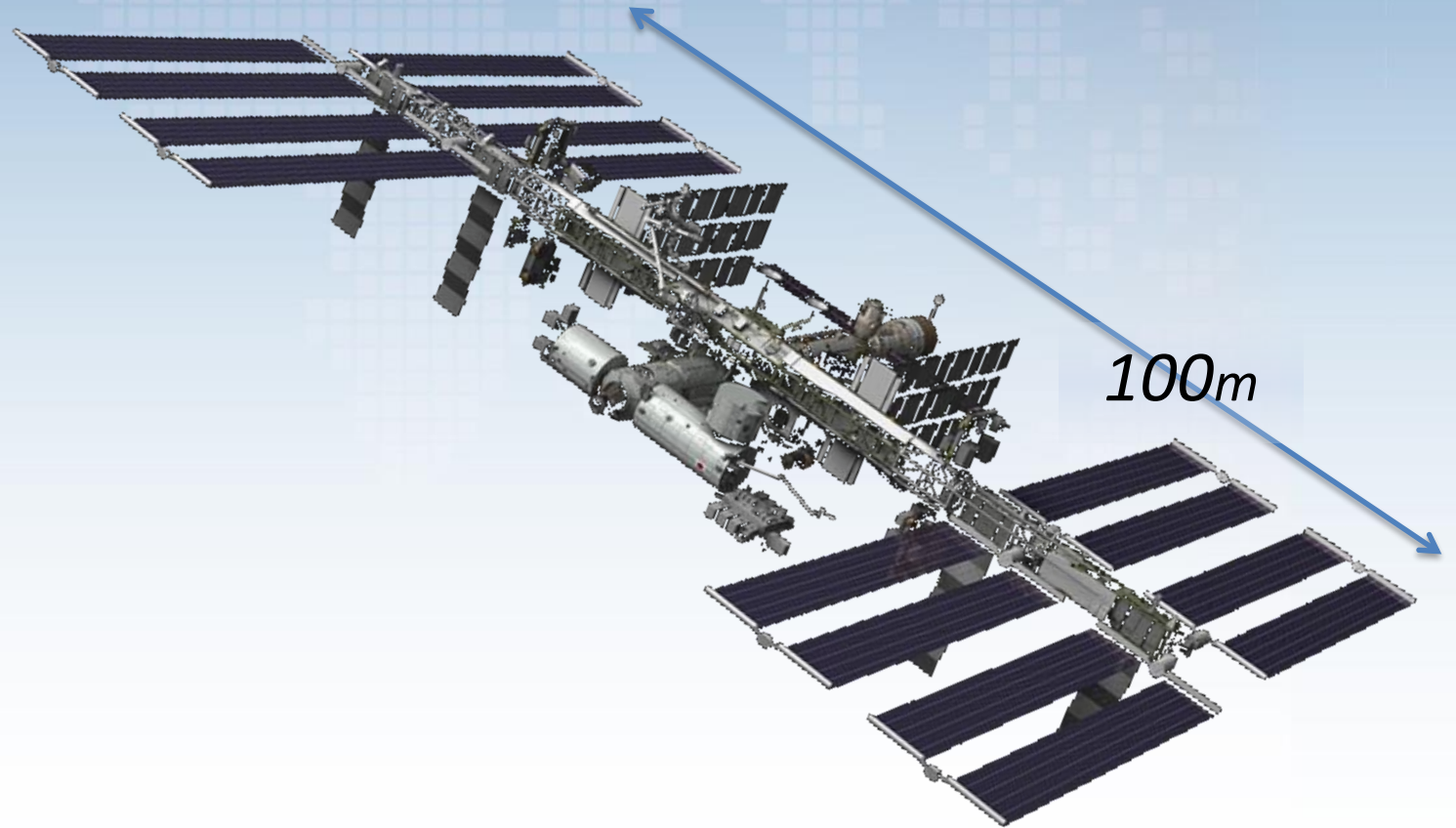
***“Security is the enabler for evolving and scaling up in a secure manner, while minimising the risk of being affected at an irrecoverable level.”***



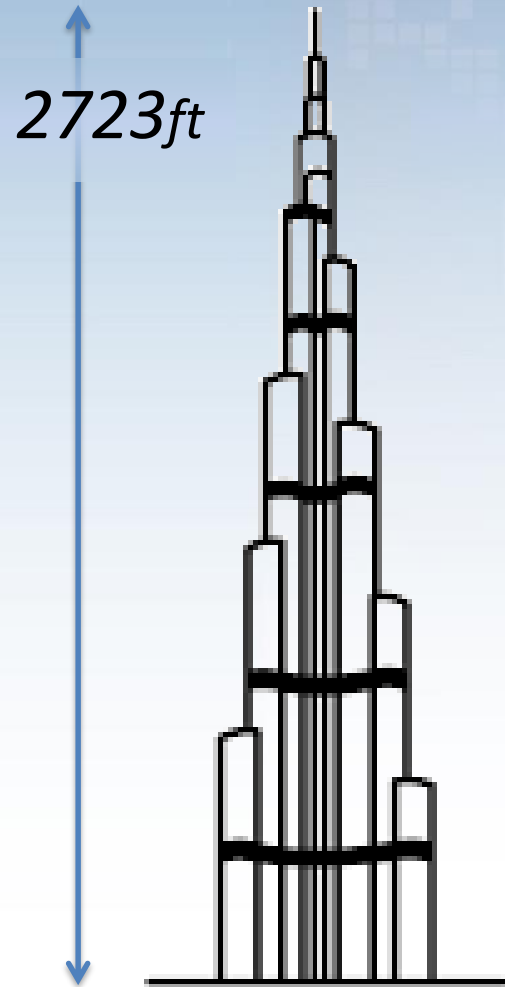
# Into perspective

**3 million** lines of software code  
on the ground support more than  
**1.5 million** lines  
of flight software code

..run on **44 computers**,  
communicating via **100 data**  
**networks**, transferring **400,000**  
**signals**

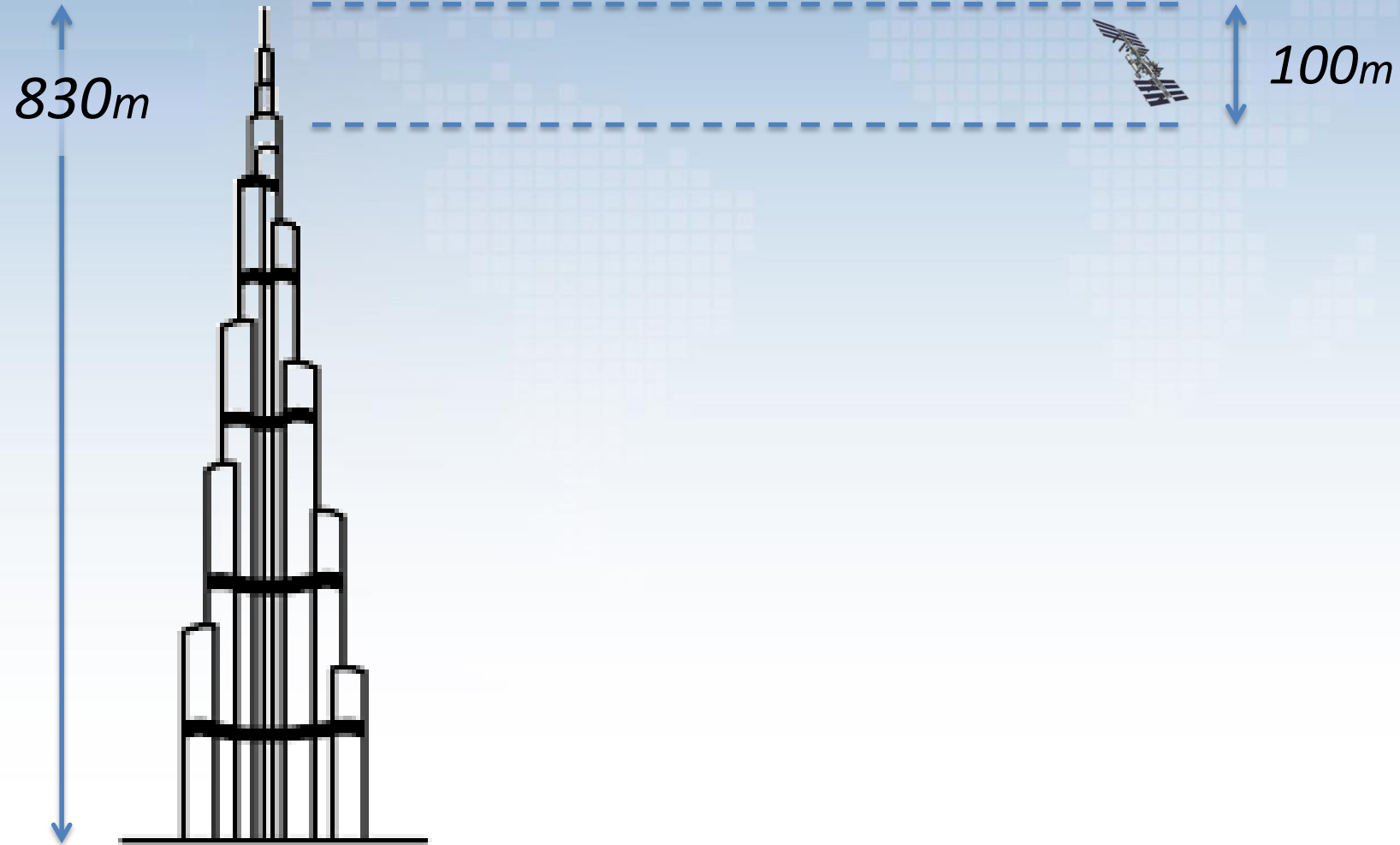


# Into perspective



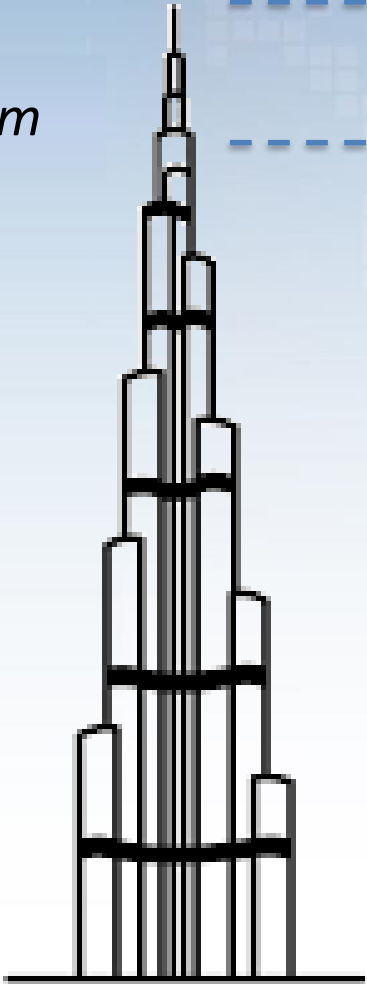
*Burj Khalifa*

# Into perspective

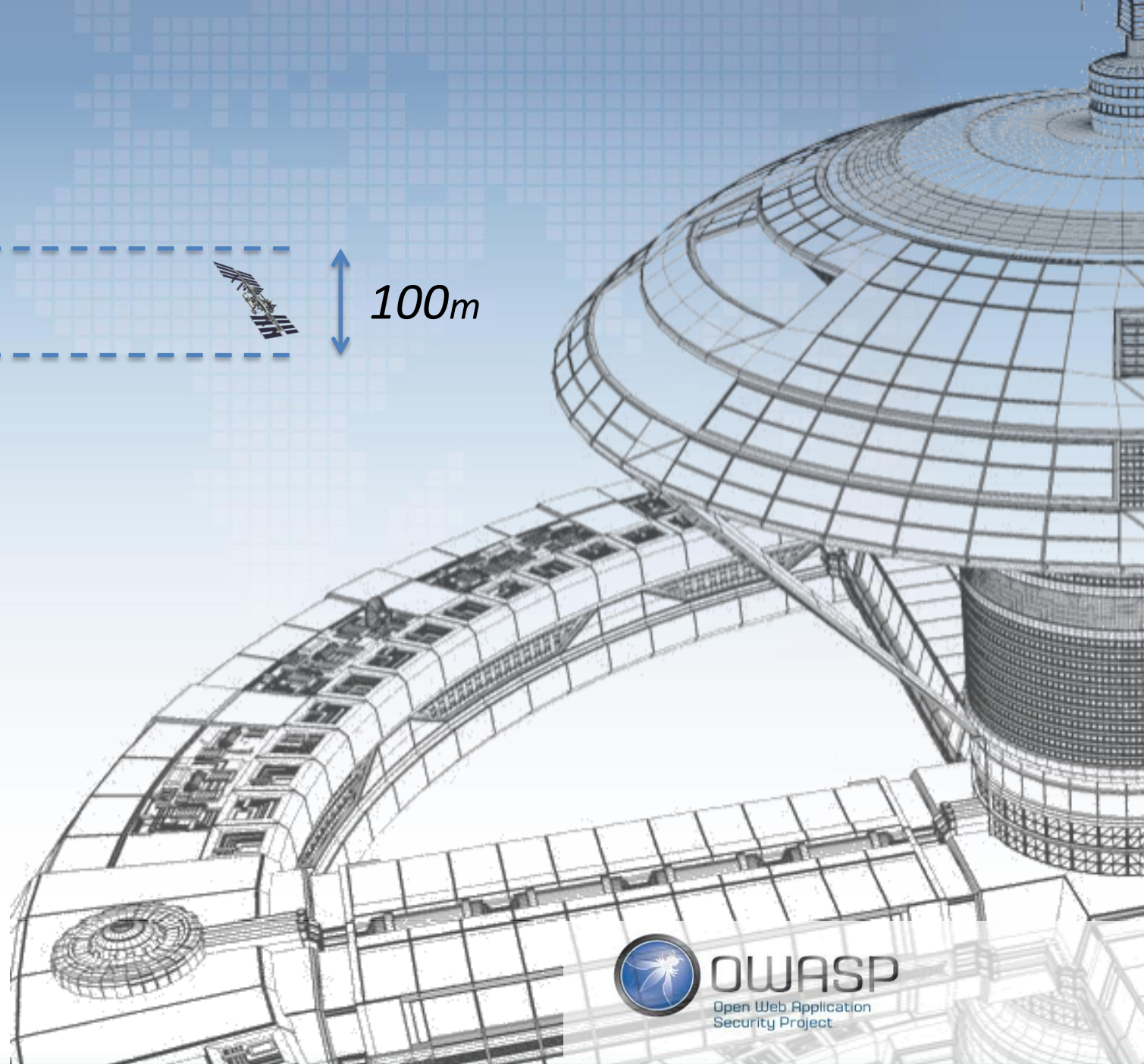


# Into perspective

830m



100m

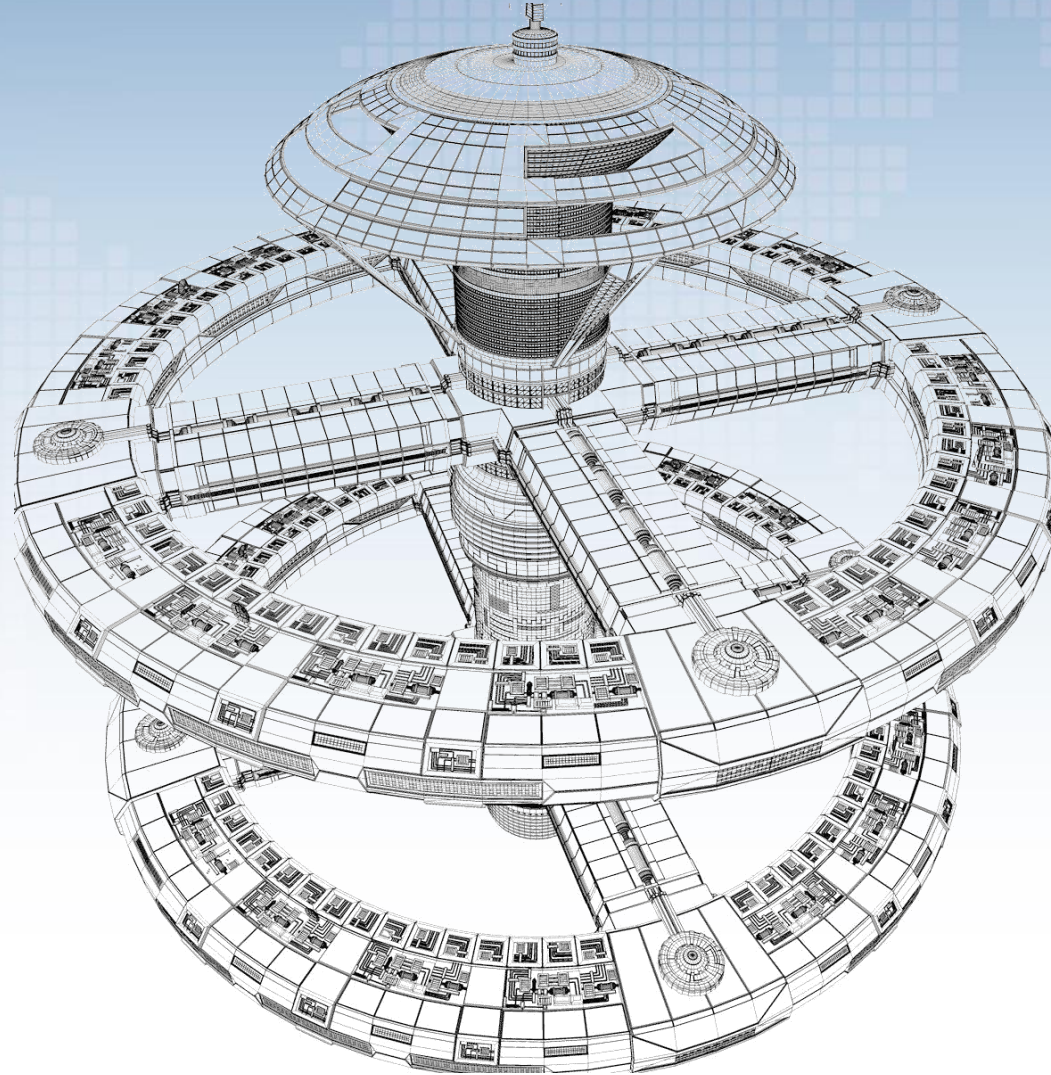



**OWASP**  
Open Web Application  
Security Project



# Into perspective

2400m





**Bloomberg  
Businessweek**  
October 8, 2018

## The Big Hack

How China used  
a tiny chip to  
infiltrate America's  
top companies



## **Dell warns of hardware Trojan**

Computer maker Dell is warning that some of its server motherboards have been delivered to customers carrying an unwanted extra: computer malware. It could be confirmation that the "hardware Trojans" ... are indeed a real threat .

- Homeland Security News Wire July 2010

## **F.B.I. Says the Military Had Bogus Computer Gear**

...the .. sinister specter of an electronic Trojan horse, lurking in the circuitry of a computer or a network router and allowing attackers clandestine access or control, was raised .. by the FBI and the Pentagon.

The new law enforcement and national security concerns were prompted by Operation CISCO Raider, which has led to 15 criminal cases involving counterfeit products bought in part by military agencies, military contractors and electric power companies in the United States.

-The New York Times, May 2008



**OWASP**  
Open Web Application  
Security Project

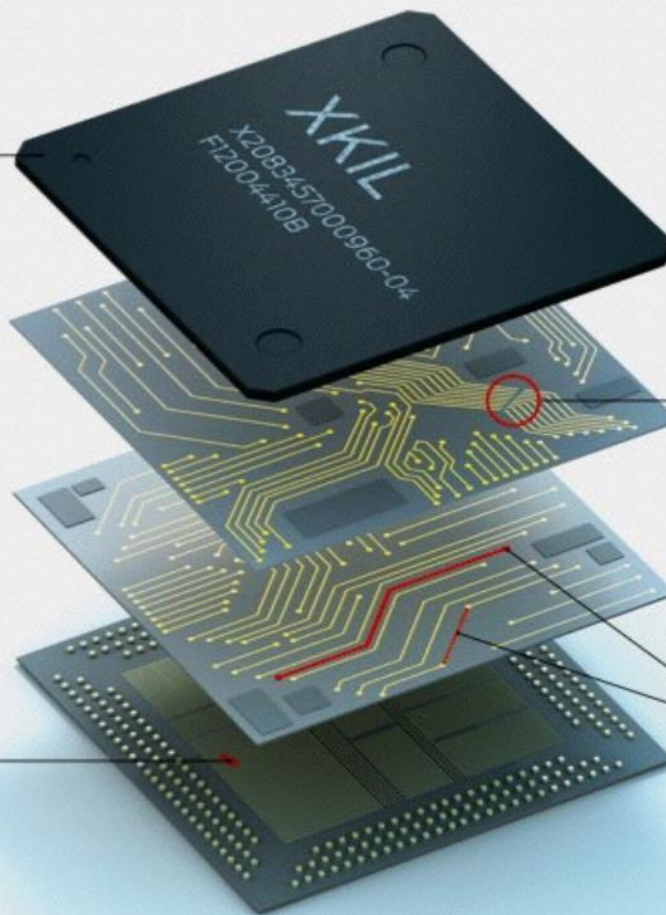


**FAKE** Counterfeiting has become a big problem for the U.S. military, and bogus packaging could disguise a questionable chip as a legitimate one. ...& **BAKE** Baking a chip for 24 hours after fabrication could shorten its life span from 15 years to a scant 6 months.



**ADD EXTRA TRANSISTORS**

Adding just 1000 extra transistors during either the design or the fabrication process could create a kill switch or a trapdoor. Extra transistors could enable access for a hidden code that shuts off all or part of the chip.



**NICK THE WIRE**

A notch in a few interconnects would be almost impossible to detect but would cause eventual mechanical failure as the wire became overloaded.

**ADD OR RECONNECT WIRING**

During the layout process, new circuit traces and wiring can be added to the circuit. A skilled engineer familiar with the chip's blueprints could reconnect the wires that connect transistors, adding gates and hooking them up using a process called circuit editing.



Massachusetts Institute of Technology



**OWASP**  
Open Web Application  
Security Project

# Security Champion



```
graph TD; SC((Security Champion)) --- S1((OWASP, OSSTMM, ISO, ENISA, NIST, PCI DSS, SANS Top 20, NCSC, EDPS, ICO, CERT-EU)); SC --- S2((Enabler)); SC --- S3((Twitter)); SC --- S4((Laws & Regulations)); SC --- S5((Developers vs Breakers)); SC --- S6((Cyber Resilience Strategy)); SC --- S7((Business RISK)); SC --- S8((Identify, Protect, Detect, Respond, Contain, Recover));
```

OWASP,  
OSSTMM, ISO,  
ENISA, NIST,  
PCI DSS, SANS  
Top 20, NCSC,  
EDPS, ICO,  
CERT-EU

Enabler

Twitter

Laws &  
Regulations

Developers  
vs Breakers

Cyber  
Resilience  
Strategy

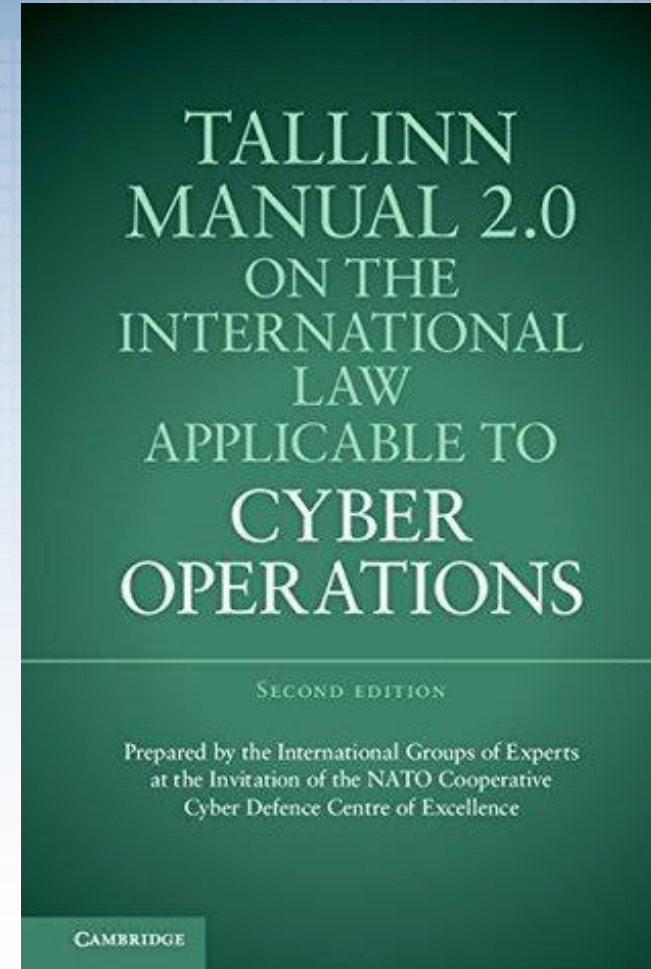
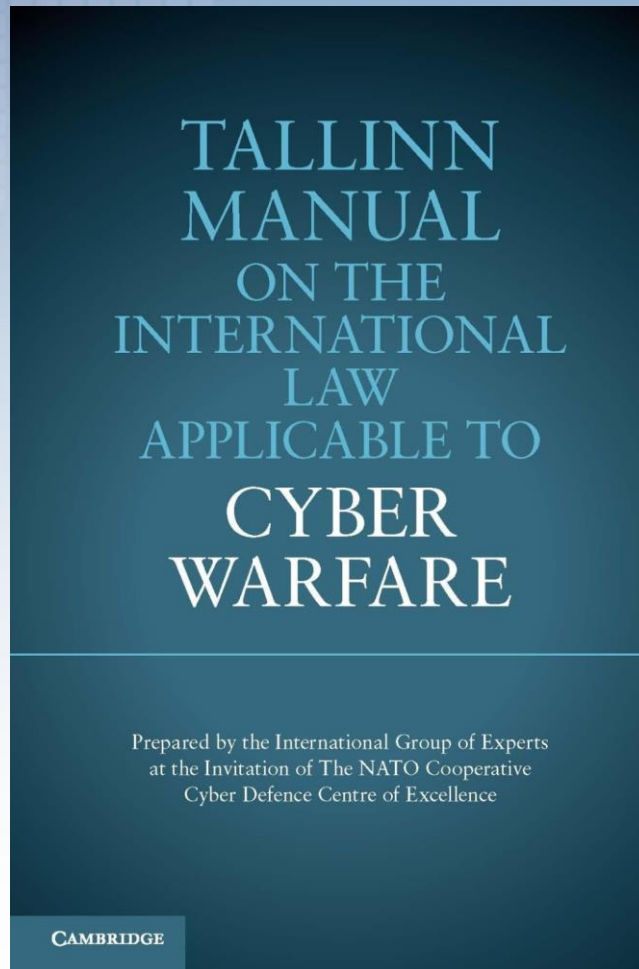
Business  
RISK

Identify  
Protect  
Detect  
Respond  
Contain  
Recover



**OWASP**  
Open Web Application  
Security Project

# #TallinnManual



***“..moved from Information Assurance to Mission Assurance.”***





**#SecurityLegend**

A red king chess piece stands prominently on a black and white checkered chessboard. In the background, several white chess pieces are visible, including a king, queen, and pawns. A red circle is superimposed on the right side of the image, containing the text 'Security Legend' in a red, serif font. The overall image conveys a sense of strategy and security.

**Security  
Legend**

# Time for Questions!



Thank you for your attention

**#OWASPLondon #CyberLondon**

 **@drgfragkos**



# "A Holistic View On Cyber Security In Evolutionary Terms (food-for-thought)"



*The Red Queen hypothesis, also referred to as the Red Queen effect, is an evolutionary hypothesis which proposes that organisms must constantly adapt, evolve, and proliferate not merely to gain a reproductive advantage, but also simply to survive while pitted against ever-evolving rival organisms in a continuously changing environment.*

*Let's explore under a Cyber lens this evolutionary hypothesis in contrast to the evolving (cyber)threats and our adaptation (as professionals) to equally evolve our Cyber Resilience capabilities (as an industry). This presentation is an opportunity to explore as professionals our security mindset and draw some personal conclusions on our Cyber Security culture in order to better ourselves. From user awareness all the way to Cyber Resilience, from developing by writing secure code to the effort it takes in breaking it, from gaps in hiring talents to hiring for the right reasons, this brief session is intended to spark a personal "eureka" moment in the mindmap of each security professional inside and outside the room.*

*by Dr. Grigorios Fragkos*

 *@drgfragkos*

Lord Ashcroft  
International  
Business  
School

Lord Ashcroft  
International Business