OSY.SSI[2015][1]

Risks, threats, adversaries

Table of Contents

A definition?

IT security invokes strategies to deal with information-related risks.

A definition?

IT security invokes strategies to deal with information-related risks.

Key terms: **Strategy**, **Dealing with**, **Risks**, **Information**.

What it's all about...

« Private information is practically the source of every large modern fortune. »

– Oscar Wilde, *An Ideal Husband*, Act I.

What it's all about...

« Private information is practically the source of every large modern fortune. »

– Oscar Wilde, *An Ideal Husband*, Act I.

Information shapes power relationships.
That is why we care about it.

Table of Contents

Risks

What is “risk”?

A *danger* (or *hazard*) is a potential event bearing undesired consequences w.r.t. a given goal:

Risks

What is “risk”?

A *danger* (or *hazard*) is a potential event bearing undesired consequences w.r.t. a given goal:

- Example : A meteor hits the Earth, destroying all forms of life.

Risks

What is “risk”?

A *danger* (or *hazard*) is a potential event bearing undesired consequences w.r.t. a given goal:

- Example : A meteor hits the Earth, destroying all forms of life.

There are many dangers: some we will meet, some we won’t.

Risks

What is “risk”?

A *danger* (or *hazard*) is a potential event bearing undesired consequences w.r.t. a given goal:

- Example : A meteor hits the Earth, destroying all forms of life.

There are many dangers: some we will meet, some we won’t.

Risk measures the expected loss caused by dangers:

$$\text{Risk} = \mathbb{E}\left[\text{cost}\right] = \sum_{\text{danger}} \text{probability of occurence} \times \text{cost}$$

Risks

What is "risk"?

A *danger* (or *hazard*) is a potential event bearing undesired consequences w.r.t. a given goal:

- Example : A meteor hits the Earth, destroying all forms of life.

There are many dangers: some we will meet, some we won't.

Risk measures the expected loss caused by dangers:

$$\text{Risk} = \mathbb{E}\left[\text{cost}\right] = \sum_{\text{danger}} \text{probability of occurence} \times \text{cost}$$

Question : what terms do we know in that equation?

Risks and threats

Risk analysis 101

Typical issues with IT?

Risks and threats

Risk analysis 101

Typical issues with IT?

- Availability

Risks and threats

Risk analysis 101

Typical issues with IT?

- Availability
- Integrity

Risks and threats

Risk analysis 101

Typical issues with IT?

- Availability
- Integrity
- Confidentiality

Risks and threats

Risk analysis 101

Typical issues with IT?

- Availability
- Integrity
- Confidentiality
- Hijacking

Risks and threats

Risk analysis 101

Typical issues with IT?

- Availability
- Integrity
- Confidentiality
- Hijacking
- etc.

Risks and threats

Risk analysis 101

Typical issues with IT?

- Availability
- Integrity
- Confidentiality
- Hijacking
- etc.

(The first three: CIA)

Risks and threats

Risk analysis 101

Typical issues with IT?

- Availability
- Integrity
- Confidentiality
- Hijacking
- etc.

(The first three: CIA)

Risk analysis is the process of:

- Identifying key dangers
- Measuring the associated cost

This results in a *risk profile*.

Note : cost might include more than money.

Risks and mitigation

Risk management 101

Facing risks, different paths can be taken:

Risks and mitigation

Risk management 101

Facing risks, different paths can be taken:

- **Avoiding** : run away. fast. don't look back.

Risks and mitigation

Risk management 101

Facing risks, different paths can be taken:

- **Avoiding** : run away. fast. don't look back.
- **Transfer** : throw the hot potato to someone else (assurance,...) ;

Risks and mitigation

Risk management 101

Facing risks, different paths can be taken:

- **Avoiding** : run away. fast. don't look back.
- **Transfer** : throw the hot potato to someone else (assurance,...) ;
- **Control** : take care of the threat (repel, fix, detect) ;

Risks and mitigation

Risk management 101

Facing risks, different paths can be taken:

- **Avoiding** : run away. fast. don't look back.
- **Transfer** : throw the hot potato to someone else (assurance,...) ;
- **Control** : take care of the threat (repel, fix, detect) ;
- **Accept** : shit happens, just pay the price.

Risks and mitigation

Risk management 101

Facing risks, different paths can be taken:

- **Avoiding** : run away. fast. don't look back.
- **Transfer** : throw the hot potato to someone else (assurance,...) ;
- **Control** : take care of the threat (repel, fix, detect) ;
- **Accept** : shit happens, just pay the price.

Each of these options has a cost.

Risks and mitigation

Risk management 101

Facing risks, different paths can be taken:

- **Avoiding** : run away. fast. don't look back.
- **Transfer** : throw the hot potato to someone else (assurance,...) ;
- **Control** : take care of the threat (repel, fix, detect) ;
- **Accept** : shit happens, just pay the price.

Each of these options has a cost.

If the risk profile is known, and **if** we know costs and solutions then we can **minimise the risk**.

Risks and threats

Criminology 101

Risks do not fall from the sky

Risks and threats

Criminology 101

Risks do not fall from the sky (well, most of the time)

Risks and threats

Criminology 101

Risks do not fall from the sky (well, most of the time)

We we almost exclusively consider *adversarial* situations, where the danger is cause by an *active, reactive, cunning* opponent trying to undermine our operations.

Risks and threats

Criminology 101

Risks do not fall from the sky (well, most of the time)

We we almost exclusively consider *adversarial* situations, where the danger is cause by an *active, reactive, cunning* opponent trying to undermine our operations.

As a consequence, risk analysis requires a good understanding of the *threat landscape* and *adversary models*.

A tentative definition

Technology is a chessboard on which people fight.

Situation

Situation

↓ Risk analysis (0)

Situation

↓ Risk analysis (0)

Risk profile

Wow. Such threat. Much risk.

Summary

Situation

↓ Risk analysis (0)

Risk profile

↓ Risk management (1)

Wow. Such threat. Much risk.

Summary

Situation

↓ Risk analysis (0)

Risk profile

↓ Risk management (1)

Action plan

Situation

↓ Risk analysis (0)

Risk profile

↓ Risk management (1)

Action plan

The performance of steps (0) and (1) is often measured by the ROI (more on that later)

Table of Contents

Refining risk analysis

In order to get a finer picture of the risk profile, we will mostly use:

- A threat exposure model
- Adversary models

(It's not perfect, but it'll help)

Threat exposure

The “No Sharks on Mt Everest principe”

A *threat* is something that produces danger.
The probability of encountering an danger is modulated by *threat exposure*.

Threat exposure

The "No Sharks on Mt Everest principe"

A *threat* is something that produces danger.
The probability of encountering an danger is modulated by *threat exposure*.

Threat exposure increases, and therefore risk increases, in situations where:

Threat exposure

The “No Sharks on Mt Everest principe”

A *threat* is something that produces danger.
The probability of encountering an danger is modulated by *threat exposure*.

Threat exposure increases, and therefore risk increases, in situations where:

- We are **close** to the threat source

Threat exposure

The "No Sharks on Mt Everest principe"

A *threat* is something that produces danger.
The probability of encountering an danger is modulated by *threat exposure*.

Threat exposure increases, and therefore risk increases, in situations where:

- We are **close** to the threat source
- We **own** something that an adversary may envy (money, IP, fame, ...)

Threat exposure

The "No Sharks on Mt Everest principe"

A *threat* is something that produces danger.
The probability of encountering an danger is modulated by *threat exposure*.

Threat exposure increases, and therefore risk increases, in situations where:

- We are **close** to the threat source
- We **own** something that an adversary may envy (money, IP, fame, ...)
- We **embody** something an adversary may despise (religion, capitalism, nuclear power...)

Threat exposure

The "No Sharks on Mt Everest principe"

A *threat* is something that produces danger.
The probability of encountering an danger is modulated by *threat exposure*.

Threat exposure increases, and therefore risk increases, in situations where:

- We are **close** to the threat source
- We **own** something that an adversary may envy (money, IP, fame, ...)
- We **embody** something an adversary may despise (religion, capitalism, nuclear power...)
- We **give in** to opportunism due to carelessness.

Threat exposure

The "No Sharks on Mt Everest principe"

A *threat* is something that produces danger.
The probability of encountering an danger is modulated by *threat exposure*.

Threat exposure increases, and therefore risk increases, in situations where:

- We are **close** to the threat source
- We **own** something that an adversary may envy (money, IP, fame, ...)
- We **embody** something an adversary may despise (religion, capitalism, nuclear power...)
- We **give in** to opportunism due to carelessness.

The risk profile can be refined to take into account a specific exposure situation, therefore enabling to better focus investments.

Threat exposure: an example

How is the IT threat landscape shaped for :

Threat exposure: an example

How is the IT threat landscape shaped for :

- Financial institutions?

Threat exposure: an example

How is the IT threat landscape shaped for :

- Financial institutions?
- Large software companies (Adobe, Google, Facebook...)?

Threat exposure: an example

How is the IT threat landscape shaped for :

- Financial institutions?
- Large software companies (Adobe, Google, Facebook...)?
- GMO-producing firms? Car companies?

Threat exposure: an example

How is the IT threat landscape shaped for :

- Financial institutions?
- Large software companies (Adobe, Google, Facebook...)?
- GMO-producing firms? Car companies?
- Nuclear plants?

Threat exposure: an example

How is the IT threat landscape shaped for :

- Financial institutions?
- Large software companies (Adobe, Google, Facebook...)?
- GMO-producing firms? Car companies?
- Nuclear plants?
- Hospitals and clinics?

Threat exposure: an example

How is the IT threat landscape shaped for :

- Financial institutions?
- Large software companies (Adobe, Google, Facebook...)?
- GMO-producing firms? Car companies?
- Nuclear plants?
- Hospitals and clinics?
- Schools, universities, museums?

Threat exposure: an example

How is the IT threat landscape shaped for :

- Financial institutions?
- Large software companies (Adobe, Google, Facebook...)?
- GMO-producing firms? Car companies?
- Nuclear plants?
- Hospitals and clinics?
- Schools, universities, museums?

Threats and adversaries

The null adversary

Not all threats can be pinned down to nefarious aims. When dealing with accidental (e.g. natural disasters, user mistake, etc.) phenomena we shall refer to the action of the *null adversary*, denoted $\perp$.

Threats and adversaries

The null adversary

Not all threats can be pinned down to nefarious aims. When dealing with accidental (e.g. natural disasters, user mistake, etc.) phenomena we shall refer to the action of the *null adversary*, denoted $\perp$.

- The null adversary has no goal, nor strategy.

Threats and adversaries

The null adversary

Not all threats can be pinned down to nefarious aims. When dealing with accidental (e.g. natural disasters, user mistake, etc.) phenomena we shall refer to the action of the *null adversary*, denoted $\perp$.

- The null adversary has no goal, nor strategy.
- It is memoryless and somewhat previsible in its actions.

Threats and adversaries

The null adversary

Not all threats can be pinned down to nefarious aims. When dealing with accidental (e.g. natural disasters, user mistake, etc.) phenomena we shall refer to the action of the *null adversary*, denoted $\perp$.

- The null adversary has no goal, nor strategy.
- It is memoryless and somewhat previsible in its actions.
- It has no special knowledge or tools.

Threats and adversaries

The null adversary

Not all threats can be pinned down to nefarious aims. When dealing with accidental (e.g. natural disasters, user mistake, etc.) phenomena we shall refer to the action of the *null adversary*, denoted $\perp$.

- The null adversary has no goal, nor strategy.
- It is memoryless and somewhat previsible in its actions.
- It has no special knowledge or tools.
- Its action is localised and temporary.

Threats and adversaries

The null adversary

Not all threats can be pinned down to nefarious aims. When dealing with accidental (e.g. natural disasters, user mistake, etc.) phenomena we shall refer to the action of the *null adversary*, denoted $\perp$.

- The null adversary has no goal, nor strategy.
- It is memoryless and somewhat previsible in its actions.
- It has no special knowledge or tools.
- Its action is localised and temporary.
- It generally makes no profit out of its actions, and doesn't have specific targets.

Threats and adversaries

The null adversary

Not all threats can be pinned down to nefarious aims. When dealing with accidental (e.g. natural disasters, user mistake, etc.) phenomena we shall refer to the action of the *null adversary*, denoted $\perp$.

- The null adversary has no goal, nor strategy.
- It is memoryless and somewhat previsible in its actions.
- It has no special knowledge or tools.
- Its action is localised and temporary.
- It generally makes no profit out of its actions, and doesn't have specific targets.

Examples : power blackout, solar storm, tsunami, fire, ageing (rust...), etc.

Threats and adversaries

The weak adversary

The weak adversary ($\star$) has minimum knowledge and means, with near-zero strategic ability.

Threats and adversaries

The weak adversary

The weak adversary ($\star$) has minimum knowledge and means, with near-zero strategic ability.

- Generally acts alone, based on easily accessible information

Threats and adversaries

The weak adversary

The weak adversary ($\star$) has minimum knowledge and means, with near-zero strategic ability.

- Generally acts alone, based on easily accessible information
- Makes meager profit

Threats and adversaries

The weak adversary

The weak adversary ($\star$) has minimum knowledge and means, with near-zero strategic ability.

- Generally acts alone, based on easily accessible information
- Makes meager profit
- Generally has no specific target and acts opportunistically

Threats and adversaries

The weak adversary

The weak adversary ($\star$) has minimum knowledge and means, with near-zero strategic ability.

- Generally acts alone, based on easily accessible information
- Makes meager profit
- Generally has no specific target and acts opportunistically

Example : a website user triggers an SQL injections involuntarily and starts exploiting it for fun.

Threats and adversaries

The strong adversary

The strong adversary (★) is often part of an organisation, it has human, legal and technical means.

Threats and adversaries

The strong adversary

The strong adversary (★) is often part of an organisation, it has human, legal and technical means.

- It builds strategies and follows them

Threats and adversaries

The strong adversary

The strong adversary (★) is often part of an organisation, it has human, legal and technical means.

- It builds strategies and follows them
- Specialised teams (up to and above 20 members)

Threats and adversaries

The strong adversary

The strong adversary (★) is often part of an organisation, it has human, legal and technical means.

- It builds strategies and follows them
- Specialised teams (up to and above 20 members)
- Gathers information from less accessible sources (dark market, reconnaissance, etc.)

Threats and adversaries

The strong adversary

The strong adversary (★) is often part of an organisation, it has human, legal and technical means.

- It builds strategies and follows them
- Specialised teams (up to and above 20 members)
- Gathers information from less accessible sources (dark market, reconnaissance, etc.).
- Potentially makes good profit out of this activity

Threats and adversaries

The strong adversary

The strong adversary (★) is often part of an organisation, it has human, legal and technical means.

- It builds strategies and follows them
- Specialised teams (up to and above 20 members)
- Gathers information from less accessible sources (dark market, reconnaissance, etc.).
- Potentially makes good profit out of this activity
- Targeted operations

Threats and adversaries

The strong adversary

The strong adversary (★) is often part of an organisation, it has human, legal and technical means.

- It builds strategies and follows them
- Specialised teams (up to and above 20 members)
- Gathers information from less accessible sources (dark market, reconnaissance, etc.).
- Potentially makes good profit out of this activity
- Targeted operations

Example : a group trying to steal and sell industrial IP.

Threats and adversaries

The strongest adversary

The strongest adversary ($\top$) has unlimited funding, is backed by expert teams, and flawless legal covers.

Threats and adversaries

The strongest adversary

The strongest adversary ($\top$) has unlimited funding, is backed by expert teams, and flawless legal covers.

- Military-grade precision and strategies
- May rely on advanced infiltration and spying operations
- Develops its own tools and gathers its own data
- Specific, high-value targets
- Almost always a government-backed and government-funded special group.

Example : the team behind Operation Aurora, targeting the largest USA-based tech firms.

Threats and adversaries: examples

Threats and adversaries: examples

- flood, cricket invasion, zombie apocalypse...

Threats and adversaries: examples

- flood, cricket invasion, zombie apocalypse...

Threats and adversaries: examples

- $\perp$ flood, cricket invasion, zombie apocalypse...
- $\star$ your occasionnal 14yo hacker, Anonymous, LulzSec...

Threats and adversaries: examples

- $\perp$ flood, cricket invasion, zombie apocalypse...
- $\star$ your occasionnal 14yo hacker, Anonymous, LulzSec...

Threats and adversaries: examples

- $\perp$ flood, cricket invasion, zombie apocalypse...
- $\star$ your occasionnal 14yo hacker, Anonymous, LulzSec...
- ★ Anunak, FIN4, Regin, El Machete...

Threats and adversaries: examples

- $\perp$ flood, cricket invasion, zombie apocalypse...
- $\star$ your occasionnal 14yo hacker, Anonymous, LulzSec...
- ★ Anunak, FIN4, Regin, El Machete...

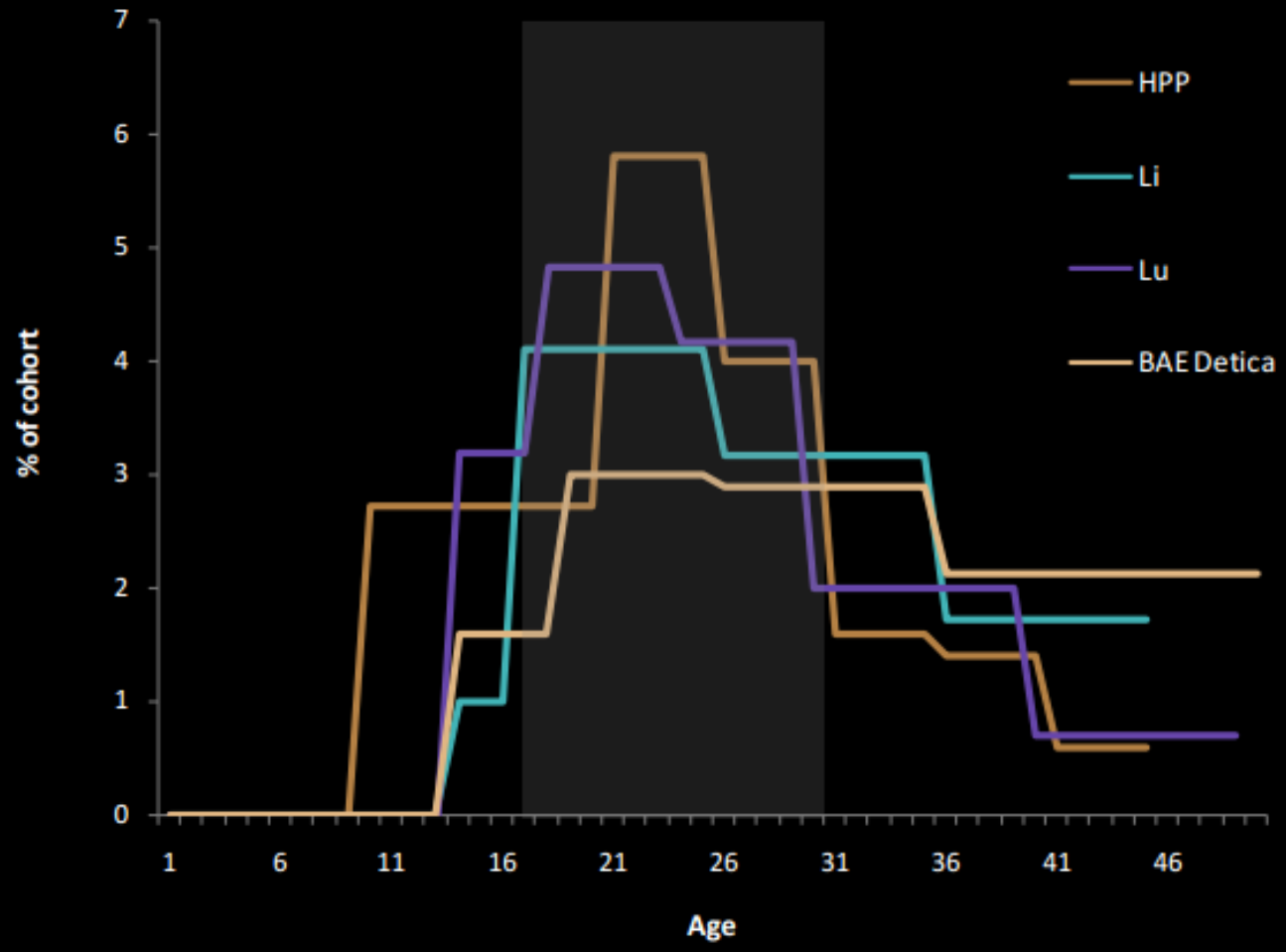
Threats and adversaries: examples

- $\perp$ flood, cricket invasion, zombie apocalypse...
- $\star$ your occasionnal 14yo hacker, Anonymous, LulzSec...
- ★ Anunak, FIN4, Regin, El Machete...
- $\top$ Unit 8200, PLA Unit 61398, NSA, OpTroy...

Threats and adversaries: examples

- $\perp$ flood, cricket invasion, zombie apocalypse...
- $\star$ your occasionnal 14yo hacker, Anonymous, LulzSec...
- ★ Anunak, FIN4, Regin, El Machete...
- $\top$ Unit 8200, PLA Unit 61398, NSA, OpTroy...

Demographics of cybercriminality



Source: UNODC elaboration of HPP, Li, Lu and BAE Detica

Table of Contents

What drives it all

What drives it all

- the micro-level, *economical incentives* $\rightarrow$ Economics

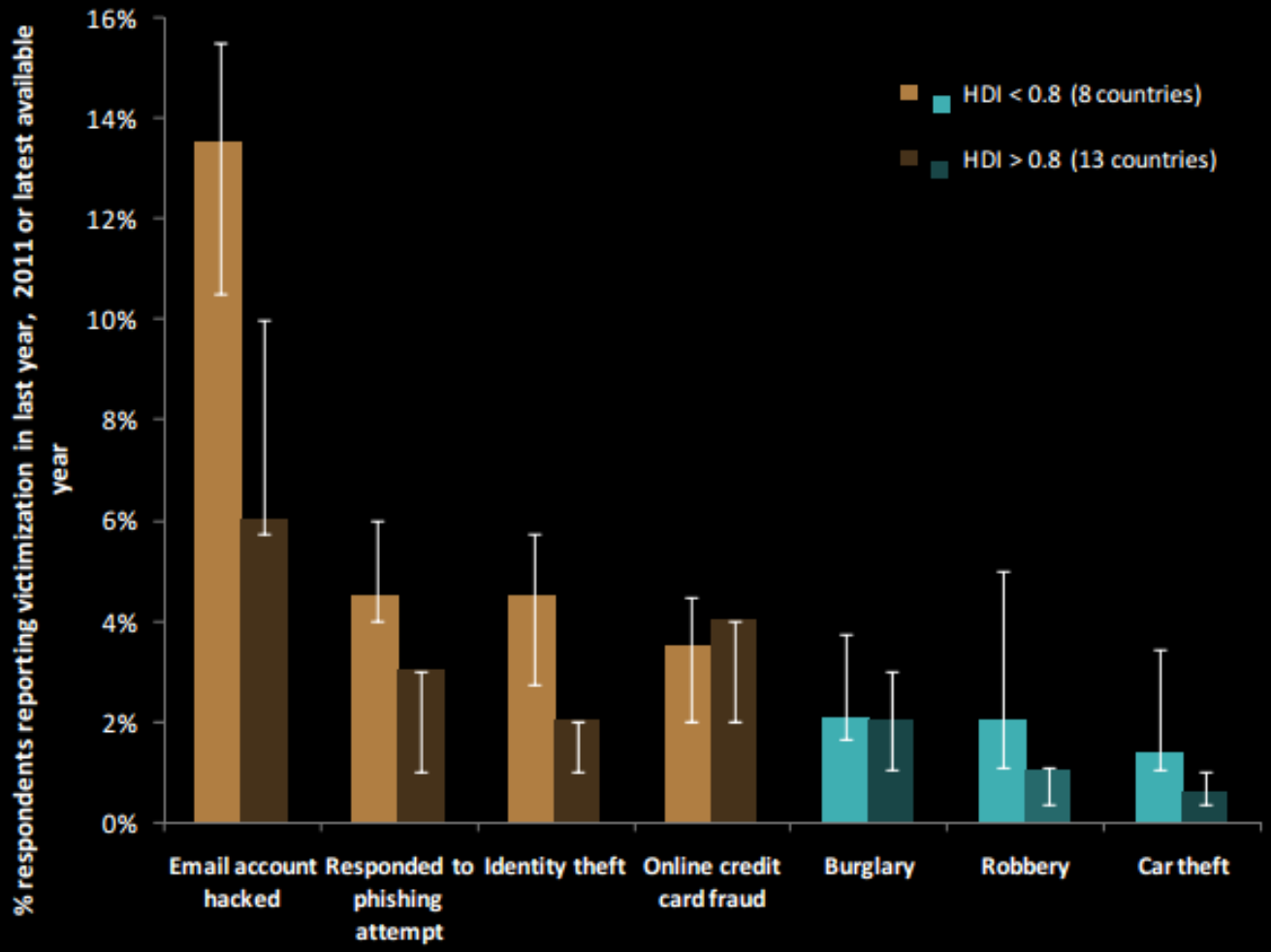
What drives it all

- the micro-level, *economical incentives* $\rightarrow$ Economics
- At the macro-level, *political goals* $\rightarrow$ Geopolitics

What drives it all

- the micro-level, *economical incentives* $\rightarrow$ Economics
- At the macro-level, *political goals* $\rightarrow$ Geopolitics

How serious is it?

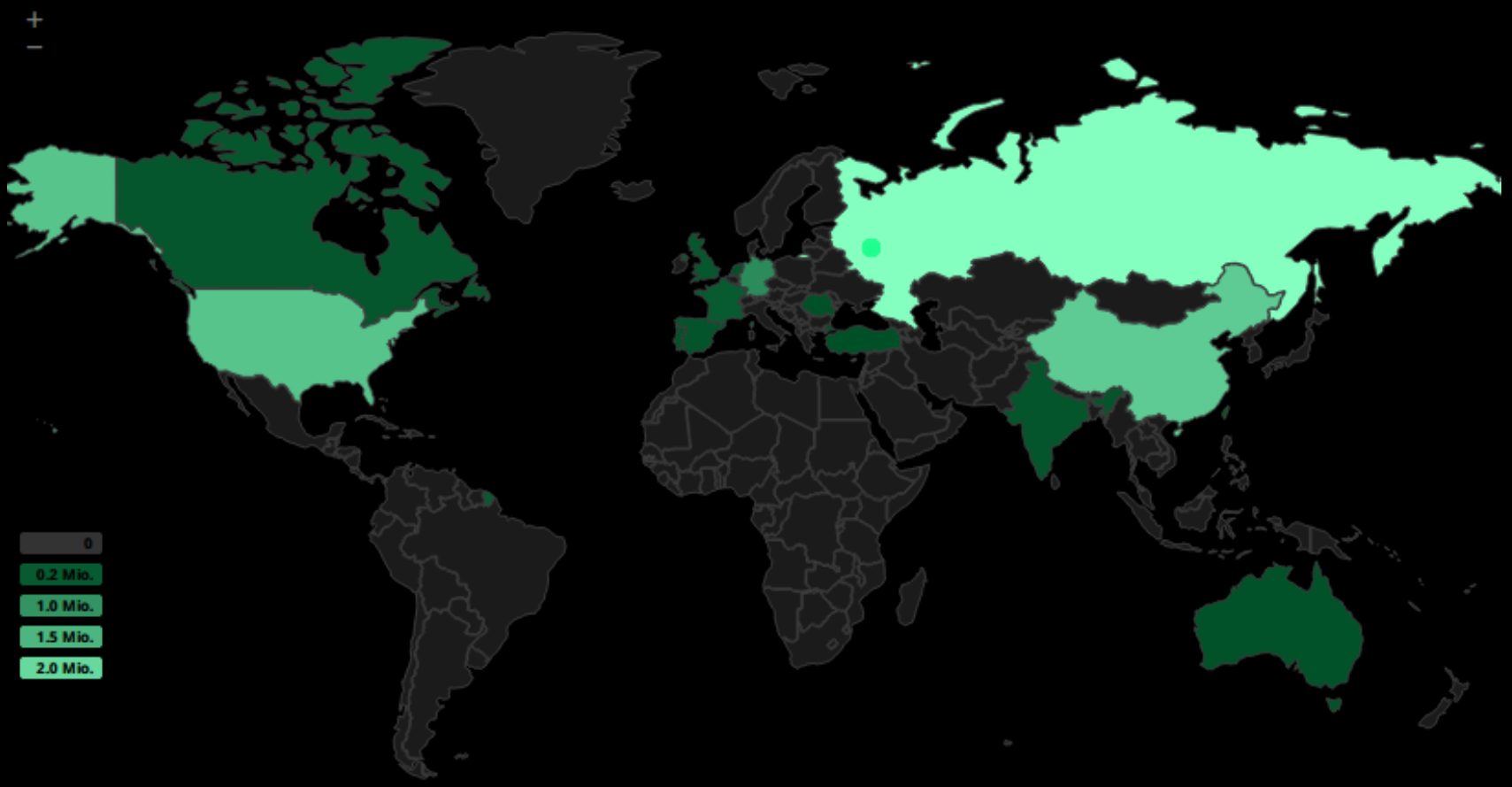


Source: UNODC elaboration of Norton Cybercrime Report and crime victimization surveys.

A good read is the *Comprehensive Study on Cybercrime*, commissioned by the United Nations.

Geopolitics

Inter-state cyberwars



Source of attacks against Germany as of 09.2014 (source : honeymap)

Inter-state cyberwars

The invisible casualties

Top 3 attackers (as of this morning, 12.01.2015):

Inter-state cyberwars

The invisible casualties

Top 3 attackers (as of this morning, 12.01.2015):

- United States

Inter-state cyberwars

The invisible casualties

Top 3 attackers (as of this morning, 12.01.2015):

- United States
- China

Inter-state cyberwars

The invisible casualties

Top 3 attackers (as of this morning, 12.01.2015):

- United States
- China
- Russian Federation

Inter-state cyberwars

The invisible casualties

Top 3 attackers (as of this morning, 12.01.2015):

- United States
- China
- Russian Federation

They also happen to be the top 3 targets.

Inter-state cyberwars

The invisible casualties

Top 3 attackers (as of this morning, 12.01.2015):

- United States
- China
- Russian Federation

They also happen to be the top 3 targets.

You can check out `http://www.digitalattackmap.com/` or `http://map.ipviking.com/` for a nice view

Two factors: covert wars and internal attacks.

Inter-state cyberwars: the most famous example

Stuxnet 2009–2011

- We will study it in details another time

Inter-state cyberwars: the most famous example

Stuxnet 2009–2011

- We will study it in details another time
- “First cyberweapon of mass destruction”

Inter-state cyberwars: the most famous example

Stuxnet 2009–2011

- We will study it in details another time
- “First cyberweapon of mass destruction”
- Unit 8200/NSA Joint operation to target Iran’s Natanz enrichment facility

Inter-state cyberwars: the most famous example

Stuxnet 2009–2011

- We will study it in details another time
- “First cyberweapon of mass destruction”
- Unit 8200/NSA Joint operation to target Iran’s Natanz enrichment facility
- Major damage, huge cost (billions of $), years to recover

Inter-state cyberwars: the most famous example

Stuxnet 2009–2011

- We will study it in details another time
- “First cyberweapon of mass destruction”
- Unit 8200/NSA Joint operation to target Iran’s Natanz enrichment facility
- Major damage, huge cost (billions of $), years to recover
- ...then it propagated beyond and that’s how we know it.

Inter-state cyberwars: the most famous example

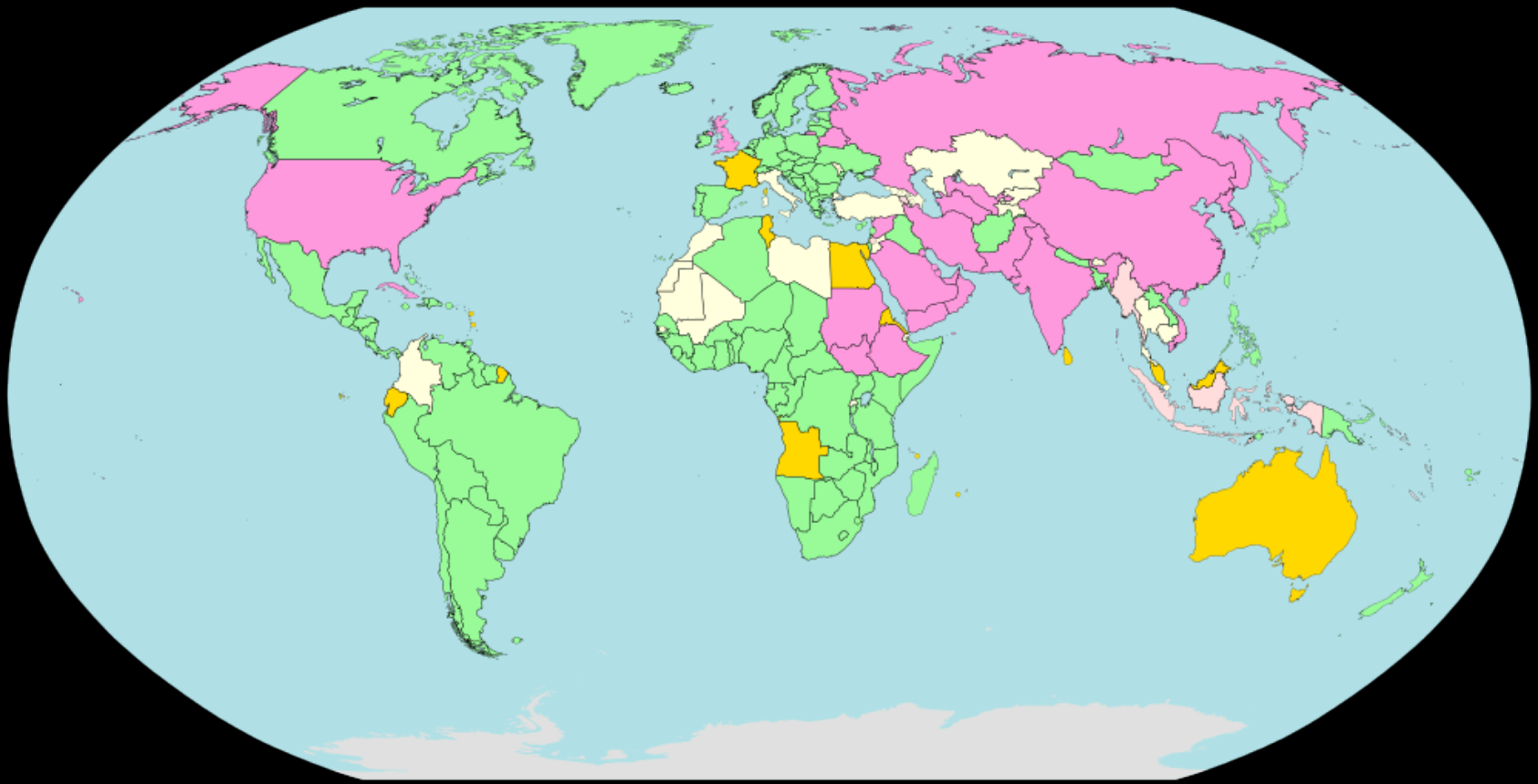
Stuxnet 2009–2011

- We will study it in details another time
- “First cyberweapon of mass destruction”
- Unit 8200/NSA Joint operation to target Iran’s Natanz enrichment facility
- Major damage, huge cost (billions of $), years to recover
- ...then it propagated beyond and that’s how we know it.

It all started with a USB stick.

Inter-state cyberwars

They are not Charlie



Hindrances to freedom of information, surveillance and censorship in 2014
(source : Reporters sans Frontières)

Debate material: privacy *vs* security

In May 2012, a WE court sentenced one of its nationals to 5 yrs

- "Participation in a criminal conspiracy for the preparation of a terrorist act."
- Prosecution presented dozens of decrypted e-mail communications of jihadist content
- Traced back to a member of a globally operating extremist group
- "translation, encryption, compression and password-protection of pro-jihadist materials"
- "taking concrete steps to provide financial support to extremist group"

The court found the required sufficient evidence to demonstrate that the defendant had provided not merely intellectual support, but also direct logistical support to a clearly identified terrorist plan.

Question : how do you feel about that?

Source: UNODC. *Use of the Internet for terrorist purposes*, 2012.