Vulnerability Handling

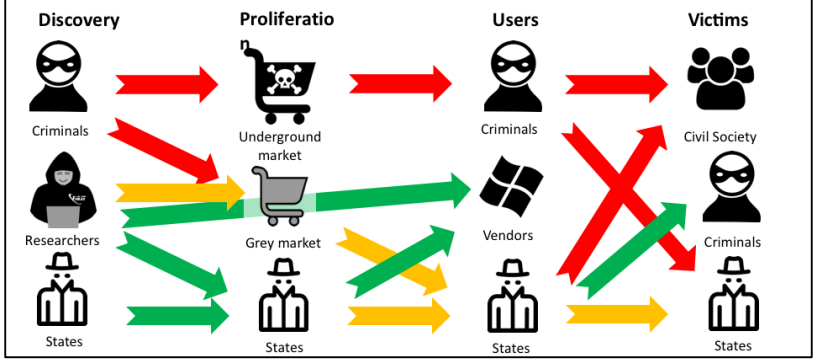
Dr. Serge Droz
Chair
serge.droz@first.org

20. January 2020

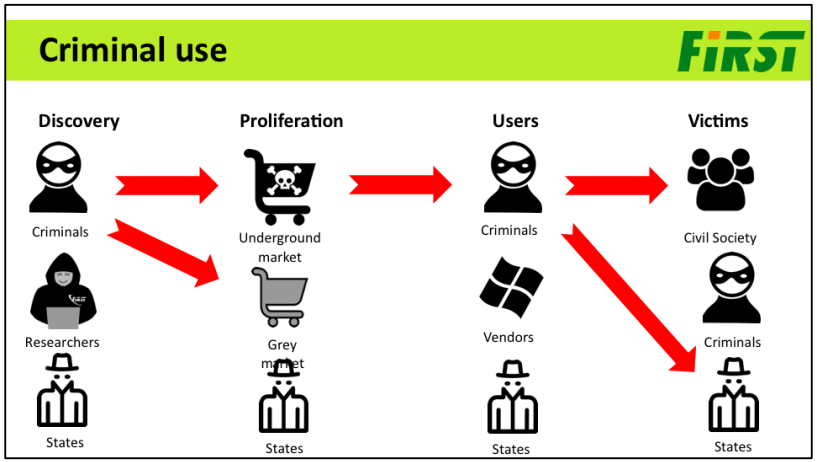
My name is Serge Droz, I'm the Chair of the Forum of Incident response and Security teams. FIRST is the global umbreall organisation bringing together more than 500 teams from over 90 countires from Government, private industry, Academia and Civil scociety.

FIRST aims at being inclusive, because we belive that the internet can only be secured in a cooperative, network-govrance, manner. FIRST member share a common goal: keeping their users safe.

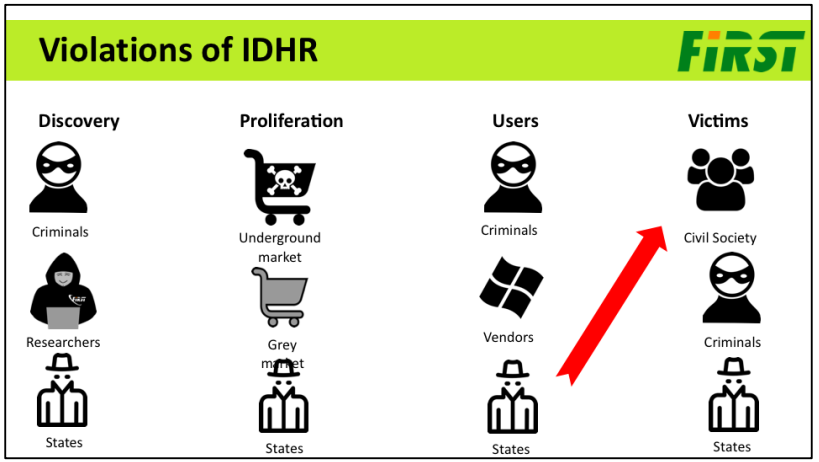
Vulnerability Ecosystem



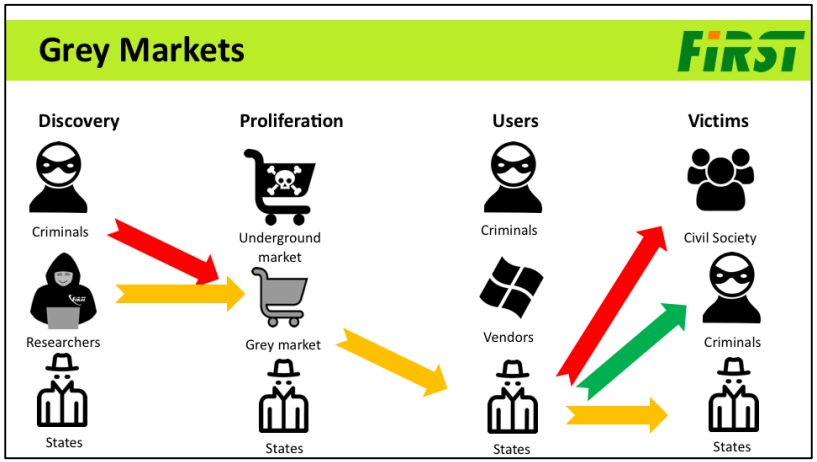
The ecosystem surrounding vulnerabilities is rather complex, and involves many stakeholders. This is a simplified view.



Combating Cybercrime needs rapid, global coordination. The only effective international treaty is the “Convention on Cybercrime” or **Budapest Convention**. Unfortunately this treaty is not universally accepted. **A law enforcement implementation of of Norm j should be sought.**



Stated attacking members of the Civil Society (there are plenty of documented examples pointing to many states) are problem. This should be covered by the **International declaration of Human rights, Article 12**.

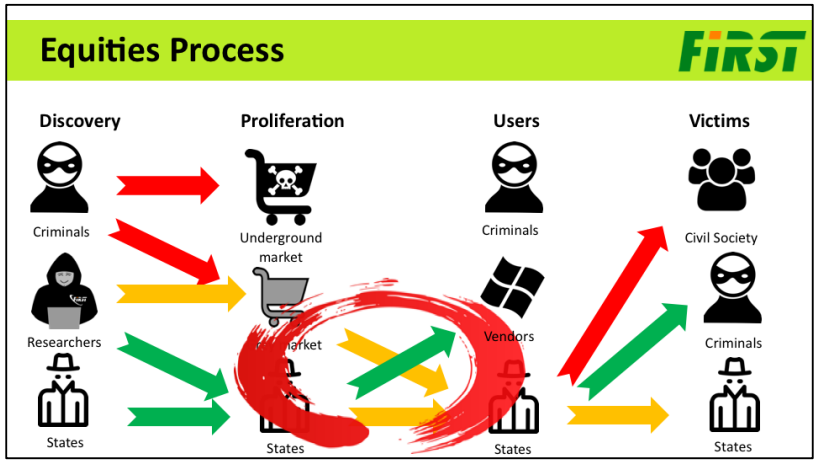


One of the big problems are grey markets. They proliferate vulnerabilities without any regards for the collateral damage. These organizations create a destabilizing market. This should be more tightly controlled, but this is not easy. An attempt to extend the Wassenaar agreement was received very critically, because many of the tools covered have legitimate uses. But the **private trading with non public vulnerabilities (0-days) should not be legal**.

https://www.lawfareblog.com/wassenaar-export-controls-surveillance-tools-new-exemptions-vulnerability-research

TL:DR: **Gray markets should not exist.**

Largest Bounty from Hacker one $250'000 compare to Zerodium: $2'500'000



Ideally states would refrain from keeping Vulnerabilities secret, but this is probably wishful thinking, despite all the harm this has already caused (Wannacry, Not Petya, Stuxnet gone out of control …).

The next best thing we can wish for is a **transparent Equities Process**. Currently there are only two published ones:

The US and the UK one. Germany seems to be in the process of creating one.

Germany reportedly wants to **codify this in law**, which is desirable.

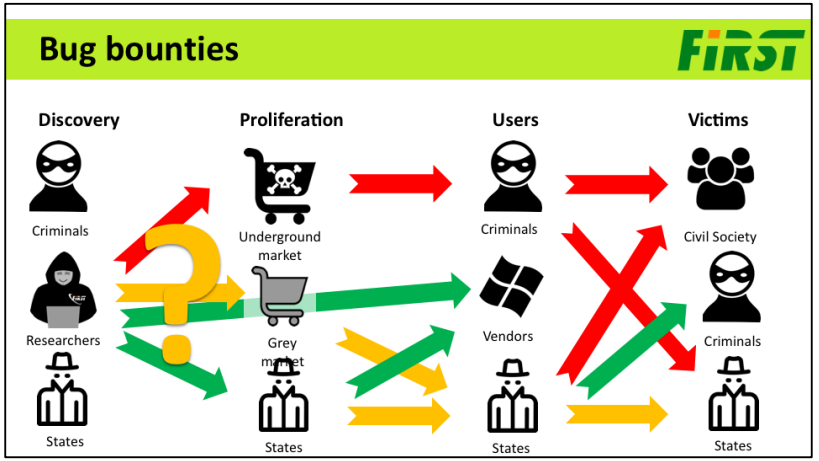
The scope of these processes is not clear. The UK process talks about results from "vulnerability research".

Vulnerabilities reported as part of a Coordinate Vulnerability Disclousure (CVD) process are typically excluded.

But states should also specify who they intend to use vulnerabilities and ensure this does not violate any of the other GGE norms (e.g. not attacking critical infrastructure,

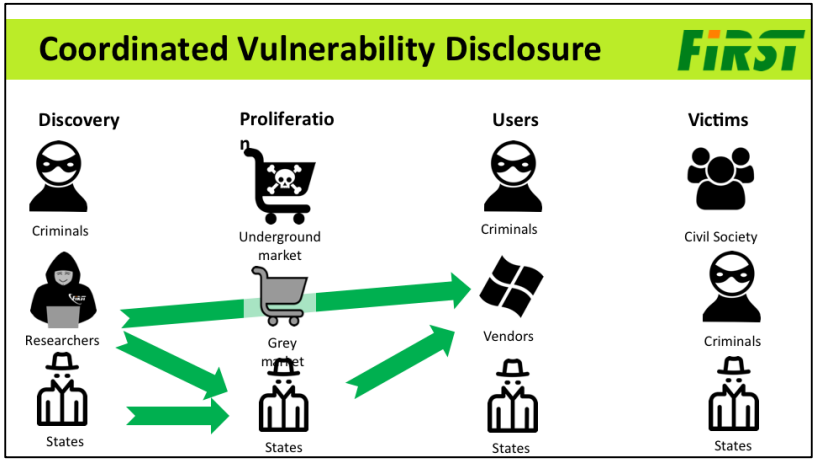
or other CSIRTs)

This only affects vulnerabilities, discovered by state actors, typically intelligence services.



Many researchers / Hackers do not have a well calibrated moral compass. One form to provide guidance are bug bounty programs. They try to incentivise responsible disclosure of vulnerabilities by awarding a price. This does not necessarily need to be a lot of money (although sometimes it is) but can simply be a token of recognition.

I refere to the presentations by Debaohra and Laurie from HackerOne.



CVD is not a simple topic. It has many players. First and foremost vendors need to be able to handle dealing with Vulnerabilities. Vendors do have a responsibility and should be held accountable if they fail. The argument, that the free market will take care of this seems to be to simplistic. So the discussion about vendor responsibility and duties needs to happen.

On the positive side, many vendors, and some national CSIRTs, today offer **bug bounties** to encourage responsible behavior.

CSIRTs play a big role in CVD. A very good example is the Dutch NCSC.nl which has a program reaching out to researchers and actively supports responsible disclosure. (I'm a fanboy of this). CSIRTs, in particular private sector CSIRTs and PSIRTs play a very important role.

Thus GGE **Norm k should apply to any CSIRTs and PSIRTs**, not only "authorized Incident Response Teams". (During a big attack who is more important: MSRC or US-CERT, no pun intended?)

In this context a big issue in in the globalized service economy are **sanctions** and

export controls. Improperly formulated they make it impossible to relay crucial information and may backfire on the issuer by leaving critical security holes open.

8

Shared responsibilities


Vendors


Researchers


States

- Vulnerabilities are a fact of life
- Improper handling undermines trust, which is a prerequisite for a functioning internet
- There are various roles and responsibilities on multiple levels to be negotiated
- This is a multi-stakeholder issue, not a state issue.

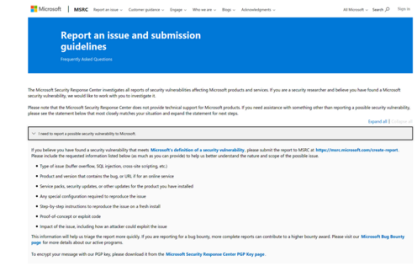
Handling Vulnerabilities is a challenge and requires to cooperation of many stakeholders. The rules are partly there but need to be sharpened and gaps need to be identified and filled.

Long term benefit should outweigh short term gain.

Vendors

Need the capability and capacity do handle vulnerabilities

- Acknowledge the fact that vulnerabilities exist
- Have a public process
- Investigate Bug Bounties
- Have a PSIRT
- Product liability?



Vendors need to take responsibility. It may well be the time to review product liability. Vendors should not be punished for vulnerabilities in their products, developing software is difficult and prone to errors. But vendors should be held accountable for their willingness and ability to handle mistakes. How long does a product need to be supported? What can we expect as minimal response? Accountability in the internet is generally very low, and vulnerability handling is no exception.

Researchers

Take an ethical stance on the work

- Acknowledge the fact that vulnerability disclosure may create harm
- Respect the challenges posed to vendors
- Realize this is not about yourself
- Education?

Researchers need to understand the wider implications of vulnerability research and in particular disclosure. It is important, that researcher understand this. States may want to invest into education and reaching out to “Hacker communities”, much like the Dutch NCSC.nl does.

In fact, it seems to me, that we have a wider issue here: I often hear of very young people being arrested for committing cyber crimes. I don’t think people get up in the morning and decide to become criminals today. Rather, it seems to me their skills and interests are not fostered and guided into the right direction. We, as societies, to this for other skills (e.g. in sports), but fail to recognize and guide IT talent.

States

Accept the Multi stakeholder nature of the Vulnerability ecosystem

- Acknowledge the wider risks of unpublished vulnerabilities
- Engage with **all** stakeholders
- Encourage responsible behavior (→ Due Diligence)
  - Maximize discourse
  - Put the equity process in the law
  - Introduce accountability for handling of non disclosed vulnerabilities
- Control export → Shut down gray markets
  Create policies that allow global CVD
- Invest in building “responsible hacker communities”

⚠ Enable CERTs to act efficiently (→ Sanctions)

Governments can play a role for good or for bad. A “free and Open Internet” requires that users can trust the internet and need not fear that they fall into security holes. Thus Vulnerabilities should be treated like dangerous weapons: The have their place in a very tightly controlled area.

Creating policy in this regard is not as easy as it seems. We need to ensure that defenders and incident responders can share information needed to secure the internet without being penalized. Sanctions or misguided export controls continue hampering the security community to effectively respond to some threats. The GGE norm k recommends that states refrain from attacking “authorized CERTs”. This is a first step. But it neglects that not only government CERTs play a crucial role but so do private sector, academic and even civil society run teams. Furthermore, if these teams cannot communicate, crucial information may net reach its destination. Holding CERTs outside the lines of fire of course comes with a price: CERTs must not be used for offensive means, and stats should ensure that this is the case.