Funded by the European Commission
Seventh Framework Programme

Cyber ROAD

Development of the Cybercrime and Cyber-terrorism Research Roadmap

Grant Agreement N. **607642**

Cybercrime and the Economy

Author(s): Jart Armin (CDF), Bryn Thompson (CDF)

Review: Przemek Jaroszewski (NASK)

CC RG-68 - Research on cybercrime economics is patchy and requires more standardization with better practices and accountability
CC RG-69 - Analysis of the threat that can be generated e.g. by new markets driven by crypto currencies

ABSTRACT

Better industry practices and accountability can help advance our knowledge of the economics of cybercrime. Knowing the true extent of the problem enables governments to budget for cost-effective measures that are fit-for-purpose. This includes the need for better prevention, detection, and application of security measures as a result of purposeful and productive research. Improving trust in the data comes from the provision of quantifiable metrics supplied by reliable sources using standardized methods that are benchmarked within the industry.

Benchmarking provides the means for a framework of accountability, whereby practices can be measured according to industry standards, and the capacity to introduce a regulatory system with managed powers of enforcement. It is already established that a barrier to the reporting of cybercrimes is a lack of trust in existing law enforcement in addition to low prosecution rates by the police. An industry based regulatory framework provides an alternative for victims to be supported, a method for action against the perpetrators and a focal point for the reporting of cybercrime.

The introduction of regulatory systems at an early stage of a newly developing cryptocurrency economy would benefit the process of cyber threat analysis and contribute towards greater accuracy in data evaluation. A system of structured regulatory measures with established cyber threat control mechanisms in place helps promote the type of environment in which an emerging cryptocurrency economy can confidently grow. An additional level of assurance is provided for consumers and the advancement of trusted and safe environments leads to the conditions in which new crypto-markets are able to flourish.

RESEARCH ACTION #1

Provide a framework for the aggregation of trusted and reliable data on the cost of cybercrime

DISTANCE TO THE MARKET: **TRL 3**
COST OF THE TOPIC: **4 STREPs + 1 IP**
AVAILABILITY OF COMPETENCE IN EUROPE: **5**
TIME SPAN FOR ADDRESSING THE ACTION: **30 months**
ACTORS: **Industry, Standardization Body, Research Institute**

What cybercrime actually costs is not yet known. Reliable data is essential for policy-making and revenue allocation from the top (governments) downwards (individual stakeholders) in order to meet the challenges of the future.

Challenges that need to be met in order to achieve this include resolving issues of trust, confusion over definitions of cybercrime, unreliable data sources, a lack of standards and benchmarks, and better information sharing.

Improved trust is co-dependent upon resolving current issues. Building upon The Budapest Convention on Cybercrime, the only international treaty to-date on cyber (enabled) crimes, would provide a first step to better definitions.

Improved methods of measurement of cybercrime for costing purposes is reliant upon the availability of accurate data. Who should provide this data and what steps are needed to ensure its accuracy?

The lack of international standards and benchmarking in the cyber security industry undermines efforts to provide consistency of data. Fast-paced innovations eclipse the processes of traditional standard-setting; fit-for purpose practices are needed.

Confusion over where and how to report cyber-attacks means incidents are under-reported which acts as an impediment to rigorous data analysis. Cross-border offending obstructs police action and adds to already low reporting rates of cybercrime.

In future scenario governments, boards and individual stakeholders can have a high level of awareness of the value of data. This is achievable through mandatory reporting of cybercrimes to a trusted entity with the data used to provide accurate analysis of the true cost of cybercrime.

RESEARCH ACTION #2

In depth threat analysis and study of preventative measures on the topic of cryptocurrencies.

DISTANCE TO THE MARKET: **TRL 4**
COST OF THE TOPIC: **5 STREPs + 0 IP**
AVAILABILITY OF COMPETENCE IN EUROPE: **4**
TIME SPAN FOR ADDRESSING THE ACTION: **36 months**
ACTORS: **Industry, Research Institute**

Different challenges are both presented and provided as new markets emerge to meet the needs of an evolving digital era. The rise of cryptocurrencies offers opportunities for better defences driven by advanced encryption and good entropy within the random number generation process.

Anticipating future threats arising out of cryptocurrency technologies is a pre-requisite with actions needed such as the early introduction of a regulatory framework for cryptocurrency operators and exchangers, which can limit the advance of decentralization.

Cybercriminals can use the lack of industry standards and best practices to their advantage as evidenced in the current situation where the true extent of cybercrime is still unknown. A framework for industry regulation of the cryptocurrency industry at an early stage of its development would ensure that challenges are faced as they unfold.

Early cross-border agreement on cryptocurrency regulations would bring legitimacy to developing systems evolving out of the virtual market. The anonymity afforded by cryptocurrencies is attractive to cybercriminals: regulation can help limit the fraud and help protect consumers.

In a future scenario cryptocurrencies are an essential feature of a vibrant economy that is trusted and secure. A regulatory framework provides a level of assurance for consumers using cryptocurrencies across a range of devices. Fraud is controlled through a number of fit-for-purpose defences aided by the provision of accurate data from trusted sources operating within a legitimate regulatory system.