CERIAS

The Center for Education and Research in Information Assurance and Security

Netherlands' Cyber Capabilities

Hans Vargas

[hvargas@purdue.edu]

Prof. Samuel Liles - CNIT581

Actor	Intentions	Skills	Targets
States	Geopolitical or improve (internal) position of power	High	Public authorities, non-governmental organisations, the business community, scientists, individuals with relevant knowledge, dissidents and opposition groups
Terrorists	Bring about social change, incite serious fear among the population or influence political decision-making	Little to moderate	Targets with high, ideological symbols
Professional criminals	Financial gain (direct or indirect)	Moderate to high	Financial products and services, IT and citizens' identity
Cyber vandals and script kiddies	Highlight vulnerabilities Hack because it's possible Prank, looking for a challenge	Little to high	Varied
Hacktivists	Ideology	Average	Varied
Internal actors	Revenge, financial gain or ideological (possibly 'controlled')	Little to high	Current or former work environment
Cyber researchers	Highlight weaknesses, improve own profile	Moderate to high	Varied
Private organisations	Obtain valuable information	Little to high	Competitors, citizens, customers
Citizens	n/a	n/a	n/a

Source: https://www.ncsc.nl/

ABSTRACT

The purpose of this study was to perform a OSINT analysis of the Netherlands capabilities to protect itself from cyber-attacks. A list of all possible and typical Actors were identified as they represent different levels of threats to this nation, the table at the left explains in detail who those actors are, what their intentions might be, the level of expertise they are expected to have, and finally the more likely targets that they might attack.
The Netherlands has a population of close to 18 million people with as estimated GDP of 696 billion USD and a per capita of 41,000 USD, which represents in the world rank, 23rd and 12th respectively. It comes as not surprise that its ICT rank is also high, occupying 7th place in the word from 2012.

This ICT level reflect the level of technology present in society, but it also has become a measure that attracts cyber attacks to its government, businesses, and citizens. There is a list of attack vectors that specifies the use of tools and technologies for cyber-attacks (not included here), but I consider more important to list the Targets that correspond to the Actors, as shown in the table to the right.
Another important subject is to list those measures in place by the Netherlands to prevent, educate, and defend themselves in the cyber domain:

- The National Cyber Security Strategy (ncsc.nl)
- National Awareness programs for local authorities, provinces, water boards, ministries and the organisations that carry out work for them.
- Security technology embracement, like migration to DNSsec, IPv6, DKIM (domainkeys identification mail signatures protocol), security development lifecycle, DigiD, etcetera.
- Cyber drills in coordination with EU, NATO, Cyber Storm IV,and @tomic 2012.
- Detection and situational Awareness
- Response Capabilities building
- Industry Cyber Reports
- Cyber operations in the Defense Sector (SCADA systems)
- Education and Investigation (NCSRA: National Cyber Security Research Agenda; the NWO: Dutch organization for Scientific Reseach)

Actors (threats)	Targets: Governments	Targets: Private organisations	Targets: Citizens
States	Digital espionage	Digital espionage	Digital espionage
	Disruption of IT (use of offensive capabilities) ★	Disruption of IT (use of offensive capabilities) ★	
Terrorists	Disruption of IT	Disruption of IT	
(Professional) criminals	Theft and sale of information ★	Theft and sale of information ★	Theft and sale of information ★
	Manipulation of information ★	Manipulation of information ★	Manipulation of information ★
	Disruption of IT	Disruption of IT ⇧	
	IT takeover	IT takeover	IT takeover
Cyber vandals and Script kiddies	Theft and publication of information ★	Theft and publication of information ★	Theft and publication of information ★
	Disruption of IT	Disruption of IT	
		IT takeover ★	
Hacktivists	Theft and publication of information ⇩	Theft and publication of information ⇩	Theft and publication of information ⇩
	Disruption of IT	Disruption of IT	Disruption of IT ⇩
		IT takeover ★	
	Defacement ★	Defacement ★	
Internal actors	Theft and publication or sale of received information	Theft and publication or sale of received information (blackmail)	
	Disruption of IT ★	Disruption of IT ★	
Cyber researchers	Receiving and publishing information	Receiving and publishing information	
Private organisations		Theft of information (business espionage) ⇧	
No actor	IT failure ⇩	IT failure ⇩	IT failure ⇩

Low	Moderate	High
No new trends or phenomena identified which result in a threat. **OR** There are (sufficient) measures available to eliminate the threat. **OR** There have been no notable incidents because of the threat during the reporting period.	New trends or phenomena identified which result in a threat. **OR** There are (limited) measures available to eliminate the threat. **OR** There have been incidents outside of the Netherlands, and a few minor incidents in the Netherlands.	There are clear developments which make the threat applicable. **OR** Measures have a limited effect, so that the threat remains considerable. **OR There have been incidents in the Netherlands.**

Key to changes: ⇧ threat has increased ⇩ threat has decreased ★ threat is new or has not been reported previously

Source: https://www.ncsc.nl/

For more information about this paper, contact Hans Vargas at hvargas@purdue.edu

CERIAS

PURDUE UNIVERSITY