Team name: CDT Mavericks
University: Royal Holloway University of London
Team members: Ela Berners-Lee, Andreas Haggman, Rory Hopcraft, Pip Thornton
Coach: Professor Keith Martin

CDT Mavericks

Decision Document

Option 1: Continuation of Policy by Other Means

An offensive policy option that targets the source of the threats.

Action	Description	Lead
Insert agents	Exploit Al Durka and NovAnoN's targeting of IT professionals to get HUMINT sources inside those organisations.	NATO
Degrade & Disrupt	Mount offensive cyber campaign against Al Durka and NovAnoN networks.	Nat'l SIGINT agencies, CYCOMs, NATO
Deny	Take down online marketplaces for attack and espionage tools by identifying and arresting hosts.	EUROPOL, INTERPOL

Option 2: Four Legs Good

A defensive policy option that focuses on robust underlying structures in society.

Action	Description	Lead
Awareness campaign	Campaign to raise awareness of ransomware, showing that hackers should be thought of as pickpockets; everyone at risk but relatively easy to keep safe.	EU
Infrastructure ranking	Identify the most crucial parts of infrastructure and prioritise their needs accordingly.	EU (EUISS)
Message control	Set up dedicated PR/communications body that organisations and companies (6) can use to advise on announcements when they have been breached.	EU
Education	Create a directive to introduce cyber security and awareness at early stage in education.	EU (EACEA)
Intelligence sharing	Centralised systematic sharing of intelligence that may impact multiple EU member states.	EU INTCEN, EUROPOL, EDA

Option 3: A Disturbance in the Force

A policy option that makes companies take responsibility for the security of supply chains and procedures and equips them with the tools to better fend off attacks.

Action	Description	Lead
Changeable passwords	Medical devices must have changeable passwords, not hard-coded. (1 & 2)	EU (ENISA)
Change passwords	Passwords on medical devices must be changed from default when installed. (5)	EU (ENISA)
Robin Hood model	Sectors identified as critical pay less/nothing for software updates (6 & 7), subsidised by other sectors paying more.	EU
Stamp out complacency	Organisations should solve security problems rather than pay ransoms.	EU

Option 4: A Balanced Diet [PREFERRED OPTION]

A balanced policy option that mixes offensive, defensive and regulatory aspects.

Action	Description	Lead
Insert agents	Exploit Al Durka and NovAnoN's targeting of IT professionals to get HUMINT sources inside those organisations.	NATO
Message control	Set up dedicated PR/communications body that organisations and companies (6) can use to advise on announcements when they have been breached.	EU
Changeable passwords	Medical devices must have changeable passwords, not hard-coded. (1 & 2)	EU (ENISA)
Change passwords	Passwords on medical devices must be changed from default when installed. (5)	EU (ENISA)
Robin Hood model	Sectors identified as critical pay less/nothing for software updates (6 & 7), subsidised by other sectors paying more.	EU (ECSEL)

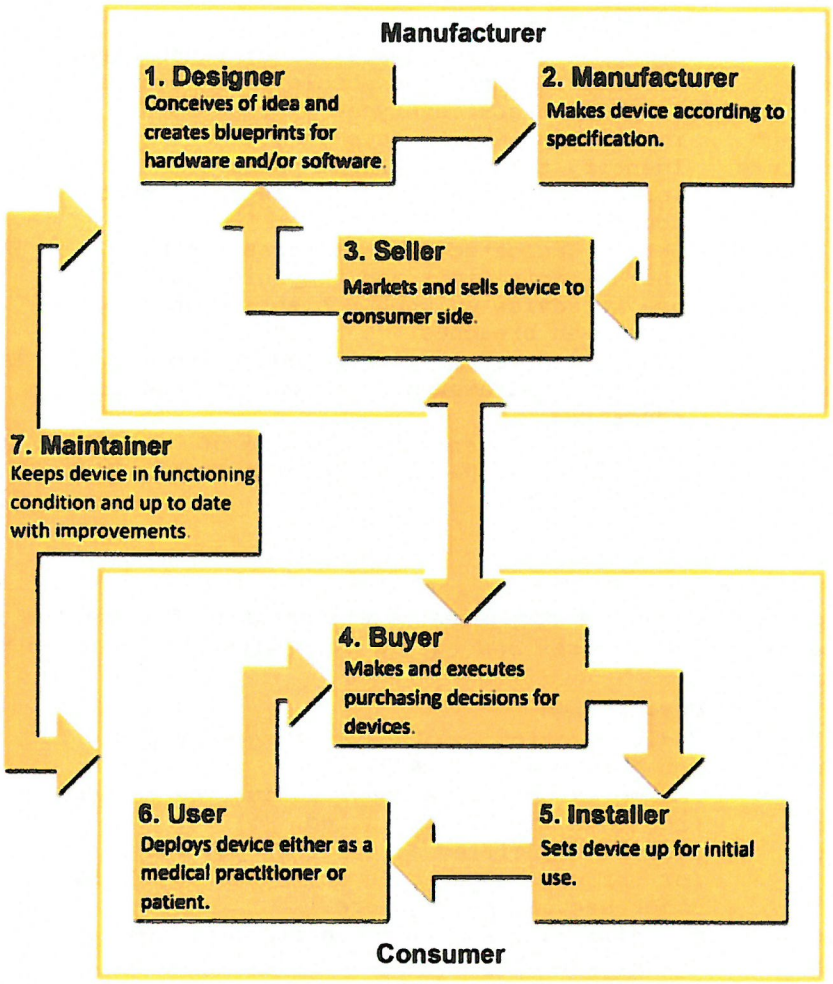


Figure 1: Medical device supply chain and lifecycle

Team name: CDT Mavericks
University: Royal Holloway University of London
Team members: Ela Berners-Lee, Andreas Haggman, Rory Hopcraft, Pip Thornton
Coach: Professor Keith Martin

CDT Mavericks

Decision Document

Option 1: Clean Digits

Seeks to improve security through user education.
Timeframe: Long-term (1 year+)
Cost: Medium

Action	Description	Lead
Awareness campaign	Target hospitals with language already used in healthcare (e.g. hygiene)	EU-OSHA
Awareness campaign	Expand to other sectors with adapted language	EU-OSHA

Option 2: The Al Capone option

Traces finances to find criminals.
Timeframe: Short-term to long-term (3 months to 1 year+)
Cost: High

Action	Description	Lead
Harness AI	Apply machine learning techniques to analyse bitcoin wallet behaviour	EUROPOL, IBM
Locate kingpin	Find NovAnoN revenue-generating streams and block them	INTERPOL, FS-ISAC

Option 3: Code monkeys

Tackles technical vulnerabilities in affected systems.
Timeframe: Immediate to long-term (2 weeks to 2 years+)
Cost: High

Action	Description	Lead
Changeable passwords	Medical devices must have changeable passwords, not hard-coded.	ENISA
Change passwords	Passwords on medical devices must be changed from default when installed.	ENISA
Robin Hood model	Sectors identified as critical pay less/nothing for software updates, subsidised by other sectors paying more.	EU
Monitor CVEs	Establish central body for monitoring new vulnerabilities.	ENISA

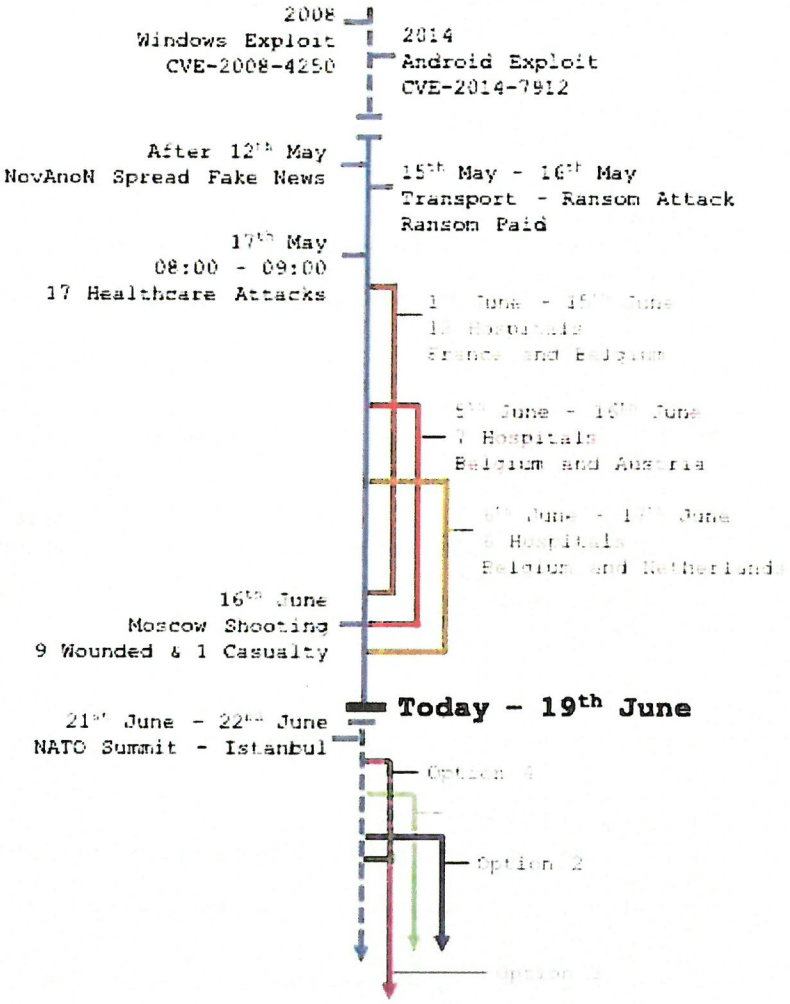
Option 4: Best of frenemies

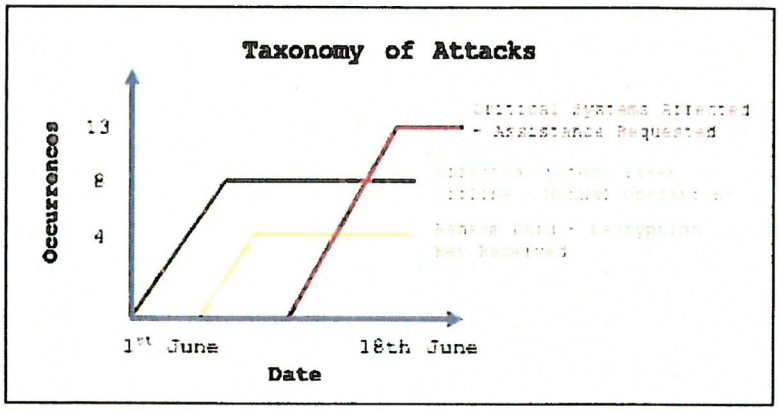
Sorts out personnel prioritisations, home and away.
Timeframe: Immediate to medium-term (2 weeks to 9 months)
Cost: Low

Action	Description	Lead
Pull rank	Prioritise saving lives over police investigations	Cabinet Ministers
HUMINT	Realign human intelligence sources already in place to reflect new information about NovAnoN organisational structure	Best-placed intel agencies

Team name: CDT Mavericks
University: Royal Holloway University of London
Team members: Ela Berners-Lee, Andreas Haggman, Rory Hopcraft, Pip Thornton
Coach: Professor Keith Martin

CDT Mavericks





Team name: CDT Mavericks
University: Royal Holloway University of London
Team members: Ela Berners-Lee, Andreas Haggman, Rory Hopcraft, Pip Thornton
Coach: Professor Keith Martin

CDT Mavericks

Written Policy Brief

FAO: Clementine Klein
Subject: Ongoing cybersecurity incidents
Priority: High

Summary:

- Ransomware attacks hit 17 European healthcare facilities and one transport infrastructure operator
- No confirmed direct fatalities or loss of service, further investigation pending.
- Low-sophistication attacks attributed to Al Durka Brigade and NovAnoN, though seem unlinked.

Details:

On **17th May** there was a **coordinated ransomware attack** targeting seventeen (17) healthcare facilities in Belgium and France. This follows reports over the past two (2) months from national and international intelligence agencies on **increased threats of terrorists using ransomware against healthcare infrastructure**. EU INTCEN reports that the prevalence of the affected devices means that **most member states are susceptible** to attack.

No immediate fatalities were caused by the attack, but EU INTCEN assesses that **casualties can be expected if attacks continue**. We agree with this assessment given the credibility of this source, although the impact of ransomware is difficult to measure because attacks often go unreported. One public study, of unconfirmed veracity, from June 2017 suggests a twelve percent (12%) increase in mortality rate during ransomware attacks and uses the deaths of two British soldiers in April 2017 as an example, although the role of ransomware in this case is denied by Army spokespersons.

The **main vulnerability** that enabled these attacks was **failure to change default passwords and unpatched software** in medical devices, particularly manufactured by GR and MacGuessin, who both command sizeable market shares. This problem has been known for several years, yet multiple factors hinder a solution:

1. Manufacturers charging for updates
2. Manufacturers not supporting older products
3. Basic cyber hygiene not being followed when installing devices
4. Hospital staff not applying available updates.

The attack has been **tentatively attributed to the Al Durka Brigade**, an offshoot of the ISIS Cyber Caliphate. Although EU INTCEN express some reservations due to differences with previous Al Durka activity, prior NATO intelligence, which we judge as reliable, shows Al Durka acquiring tools for attacks on medical facilities which are lucrative sources of income. Ransomware attacks represent an attempt by ISIS to **diversify sources of revenue** among setbacks to their traditional funding avenues.

In a separate incident on **16th May**, Berlin **train operator BVG** suffered a ransomware attack affecting its payment systems. BVG themselves think they were **not specifically targeted**, but caught in a widespread attack **perpetrated by Anonymous splinter group NovAnoN**. Although there was **no disruption to train operations**, BVG suffered financial loss. We conclude that poor cyber hygiene affects several critical infrastructure sectors.

The BVG attack stopped only when the €100,000 ransom was paid. Ransom payments have also been made in previous attacks on healthcare, suggesting the problem is only being solved superficially and **deeper security problems are not being addressed.**

At this stage **we assess that the links between the attacks are tenuous,** and the attacks are therefore unrelated. The evidence linking the two groups is circumstantial and the motives of the groups differ: Al Durka's motives are economic, while NovAnoN's are social and political.