ST Electronics
Info-Security
A member of ST Engineering

ICTA
ideas actioned

SRI LANKA
CERT|CC

Role of NCSOC and Implications

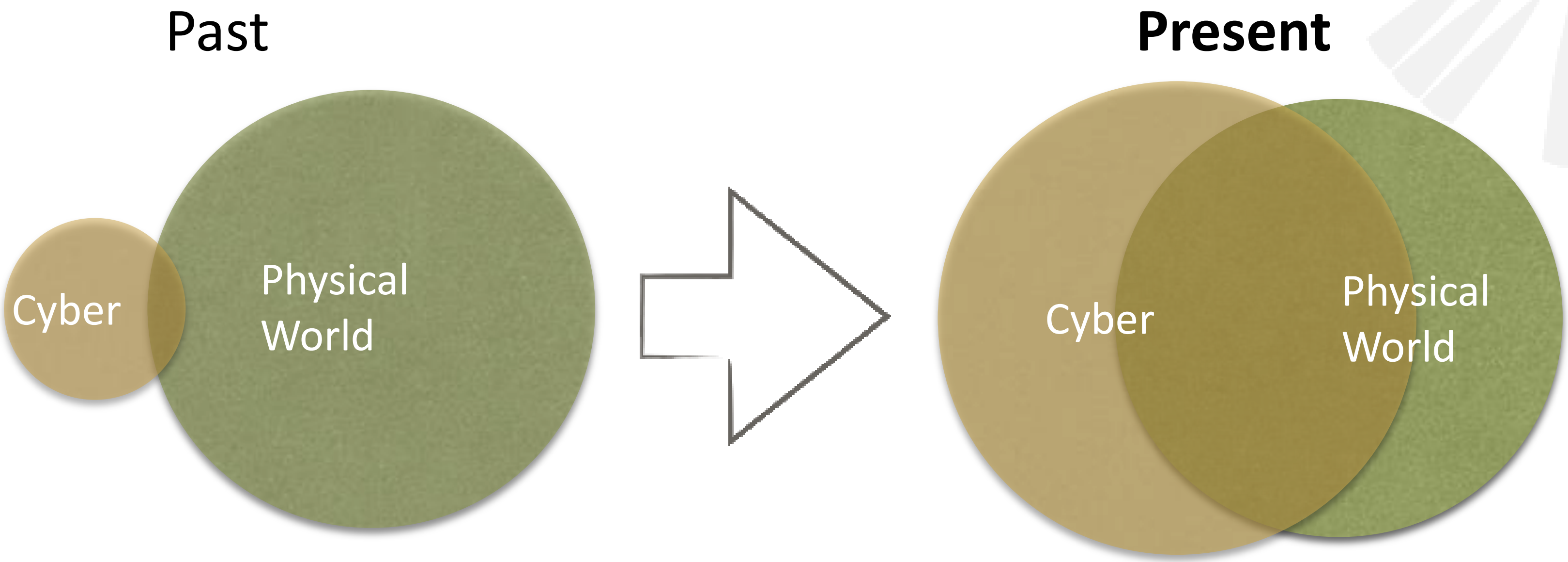
Presented by:

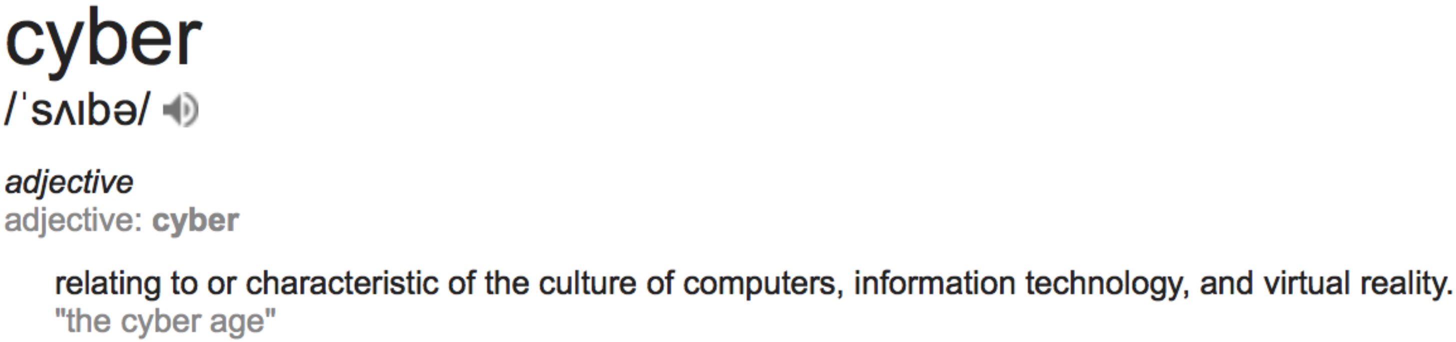
Goh Eng Choon
General Manager
27 April 2017

ENGINEERING
WITH PASSION

Empowering thru' Innovation

Change In Landscape




cyber

/ˈsʌɪbə/

adjective

adjective: **cyber**

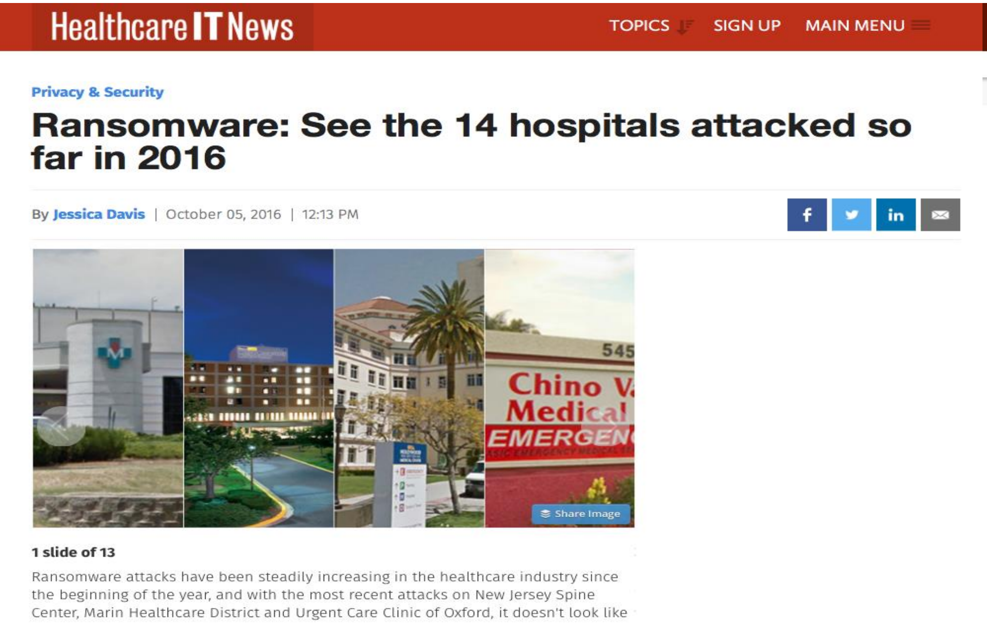
relating to or characteristic of the culture of computers, information technology, and virtual reality.

"the cyber age"

Why Cyber Attacks are the way to go?

- The Cyber & Physical worlds are very connected.
- Cheaper than conventional warfare.
- Difficult to attribute source(s) of attacks.
- Levelled playing field for threat actors with less physical arsenal & man-power.

Actual Incidents



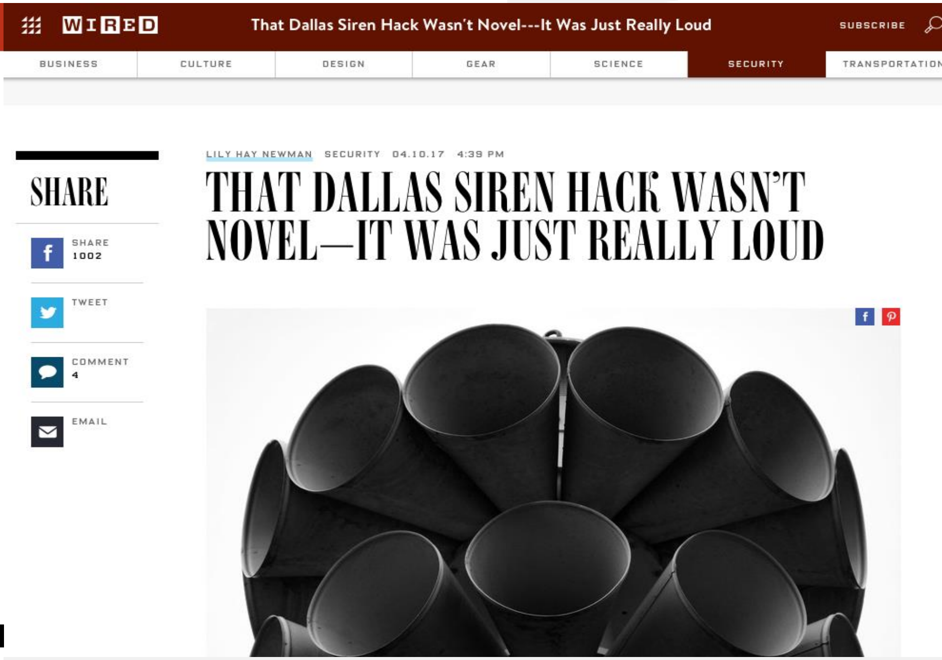
Privacy & Security

Ransomware: See the 14 hospitals attacked so far in 2016

By Jessica Davis | October 05, 2016 | 12:13 PM

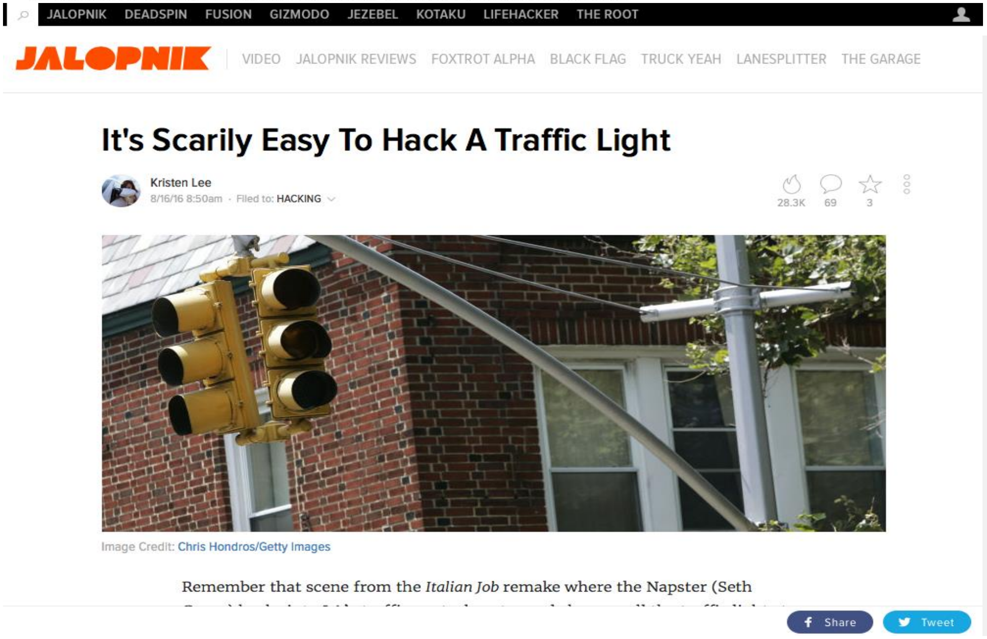
1 slide of 13

Ransomware attacks have been steadily increasing in the healthcare industry since the beginning of the year, and with the most recent attacks on New Jersey Spine Center, Marin Healthcare District and Urgent Care Clinic of Oxford, it doesn't look like



LILY HAY NEWMAN SECURITY 04.10.17 4:39 PM

THAT DALLAS SIREN HACK WASN'T NOVEL—IT WAS JUST REALLY LOUD

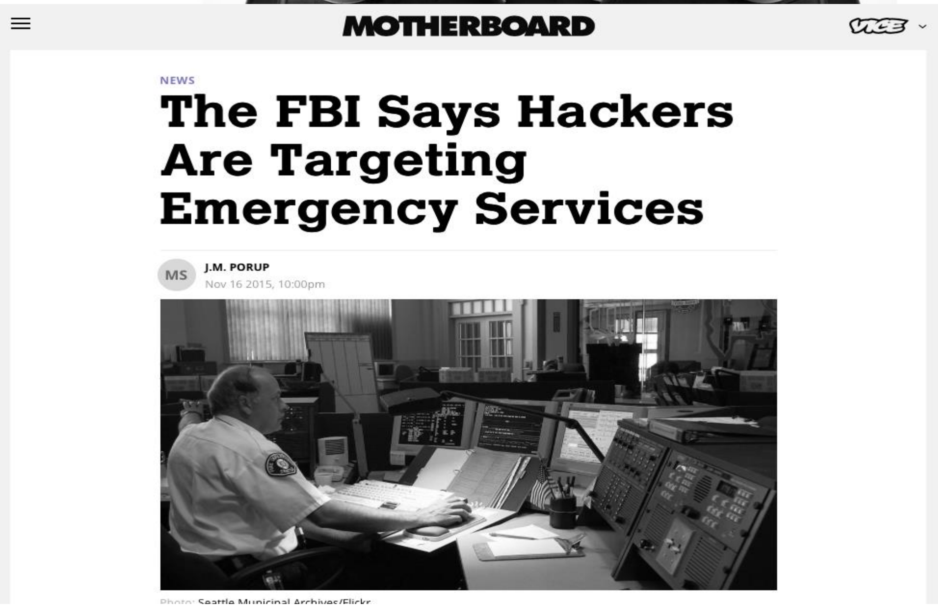


It's Scarily Easy To Hack A Traffic Light

Kristen Lee
8/16/16 8:50am · Filed to: HACKING

Image Credit: Chris Hondros/Getty Images

Remember that scene from the *Italian Job* remake where the Napster (Seth



NEWS

The FBI Says Hackers Are Targeting Emergency Services

MS J.M. PORUP
Nov 16 2015, 10:00pm

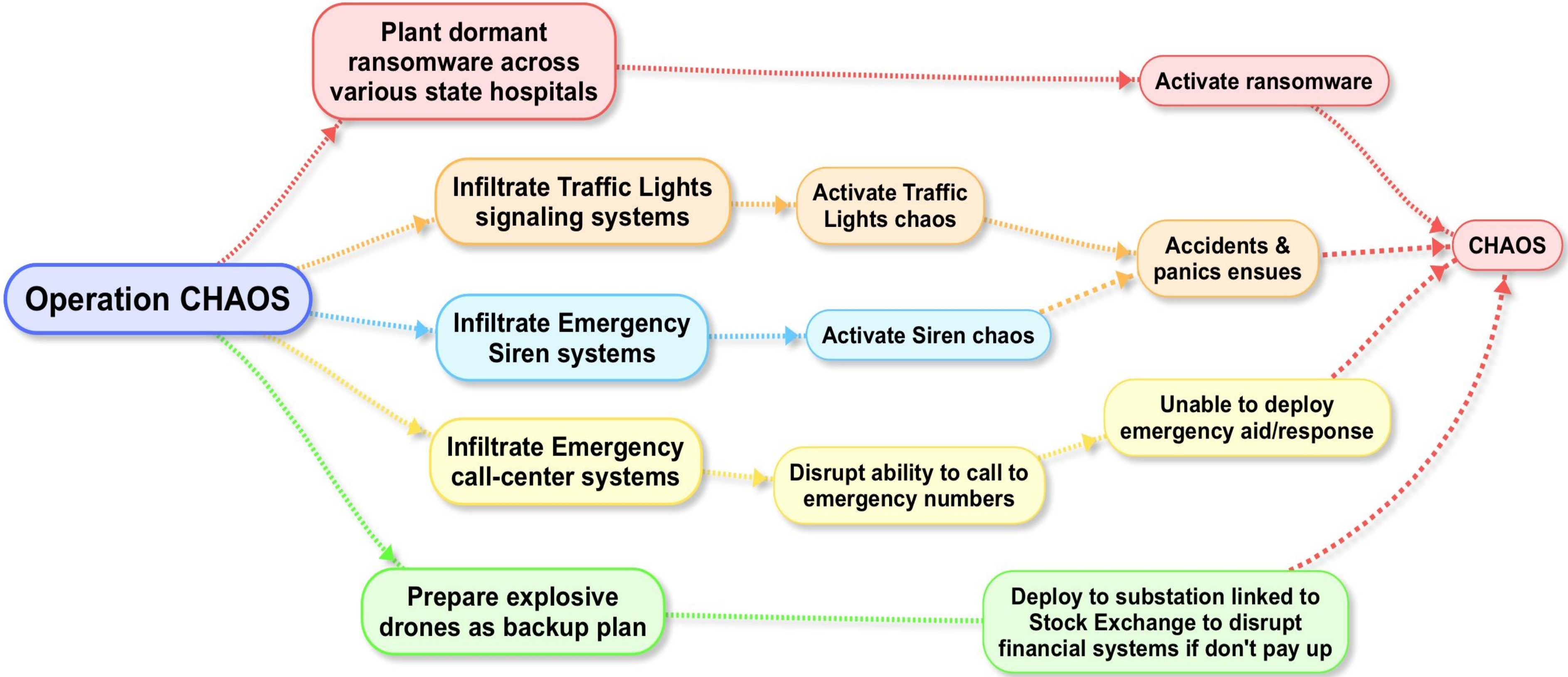
Photo: Seattle Municipal Archives/Flickr

What Exactly is Cyber Warfare?

- Instead of isolated incidents across different places…

- Imagine well-trained (~~funded~~) & motivated extremist groups decide to string these into one organised operation. Lets call it OPERATION CHAOS.

IT IS **NOT** A MATTER IF IT CAN HAPPEN,
IT IS A MATTER OF WHEN….



Operation CHAOS

Plant dormant ransomware across various state hospitals

Activate ransomware

Infiltrate Traffic Lights signaling systems

Activate Traffic Lights chaos

Accidents & panics ensues

Infiltrate Emergency Siren systems

Activate Siren chaos

Infiltrate Emergency call-center systems

Disrupt ability to call to emergency numbers

Unable to deploy emergency aid/response

Prepare explosive drones as backup plan

Deploy to substation linked to Stock Exchange to disrupt financial systems if don't pay up

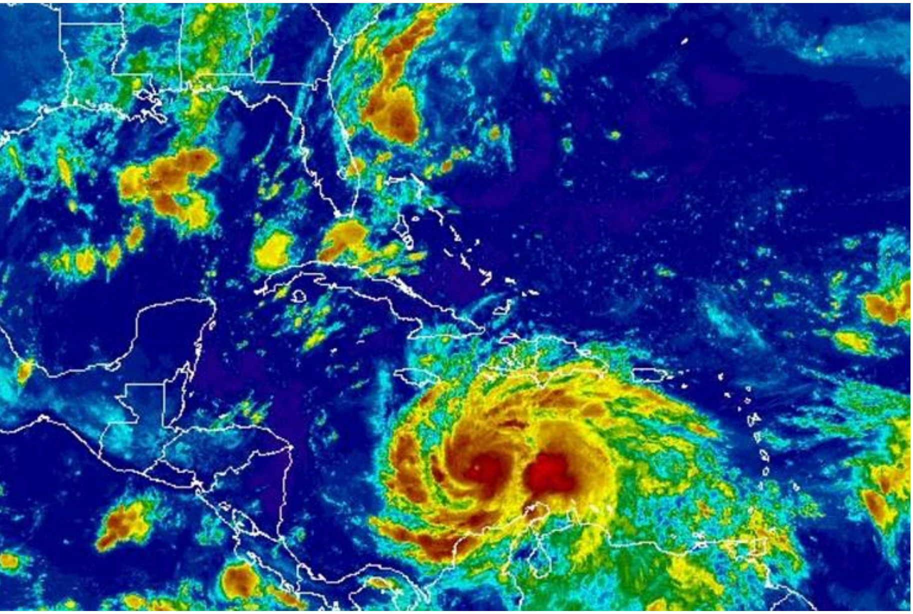
CHAOS

WITHOUT A NCSOC……..

- **THIS IS ONE BIG DISASTER - To a National Emergency Coordination Agency.**
- **POOR SITUATIONAL AWARENESS**
  In terms of Critical Cyber-Physical Systems health state.
- **CHAOS IS GUARANTEED - With Emergency Call Handling System disrupted.**

SO WHAT DIFFERENCE WILL A NATIONAL CYBER SECURITY OPERATION CENTRE MAKE?

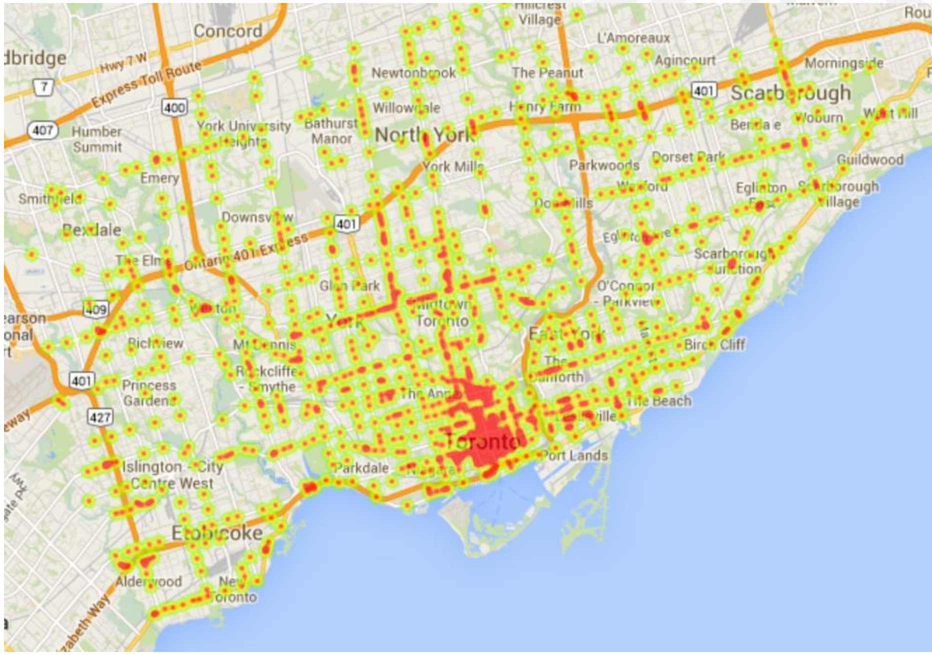
Early Warning



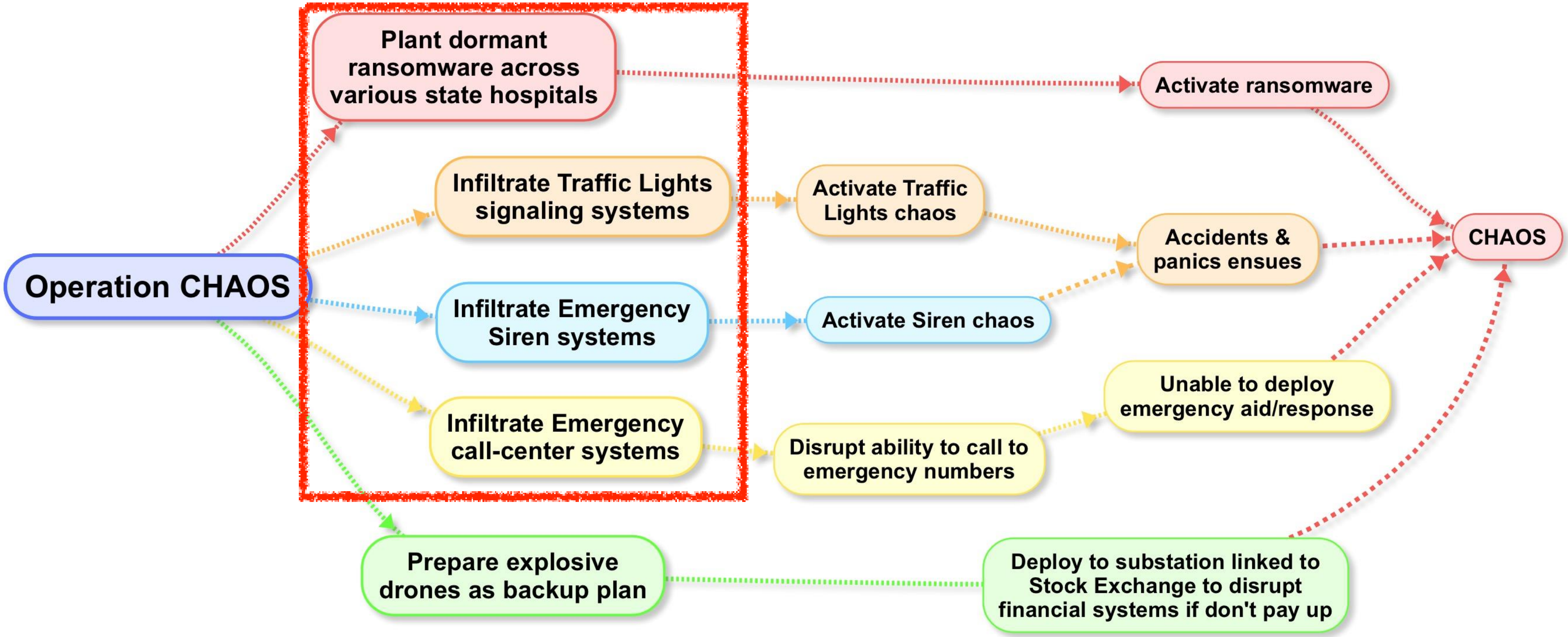
Physical World

Cyber World

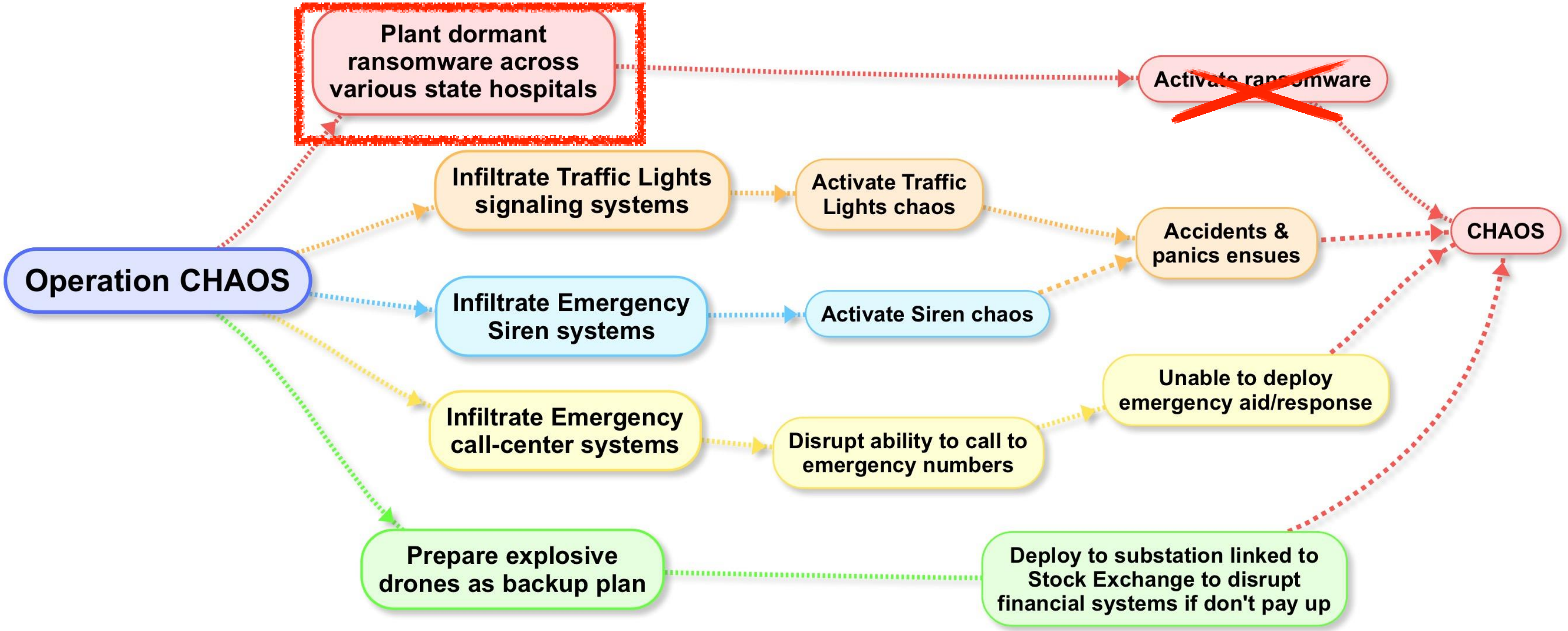
Situational Awareness



Organisational Level **National Level**


Plant dormant ransomware across various state hospitals
Activate ransomware
Infiltrate Traffic Lights signaling systems
Activate Traffic Lights chaos
Accidents & panics ensues
CHAOS
Operation CHAOS
Infiltrate Emergency Siren systems
Activate Siren chaos
Unable to deploy emergency aid/response
Infiltrate Emergency call-center systems
Disrupt ability to call to emergency numbers
Prepare explosive drones as backup plan
Deploy to substation linked to Stock Exchange to disrupt financial systems if don't pay up

- A National CSOC ingests alerts from critical sectors’ sensors.
- Highly unlikely that every intrusion attempts have perfect evasion.
- Provides EARLY warning & overall Situational Awareness.
- MUST collaborate with Intelligence & Crisis Coordination agencies.



Operation CHAOS

Plant dormant ransomware across various state hospitals

~~Activate ransomware~~

Infiltrate Traffic Lights signaling systems

Activate Traffic Lights chaos

Accidents & panics ensues

CHAOS

Infiltrate Emergency Siren systems

Activate Siren chaos

Infiltrate Emergency call-center systems

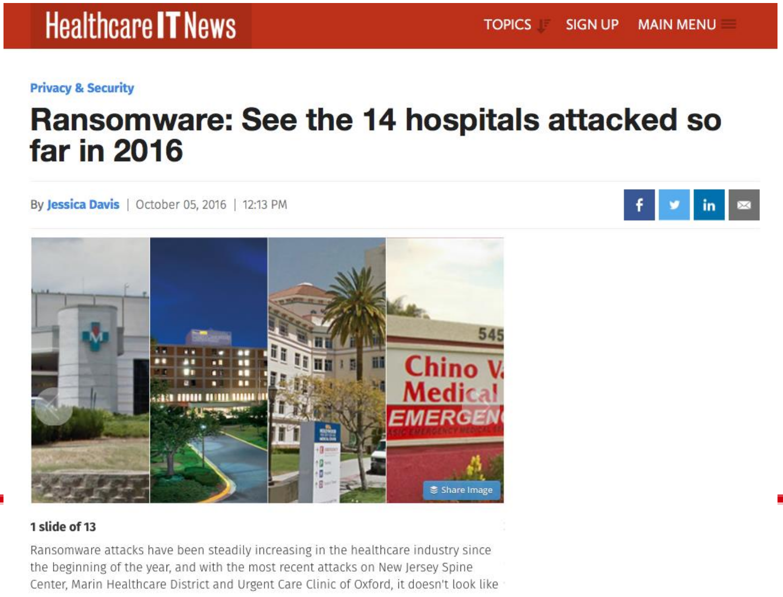
Disrupt ability to call to emergency numbers

Unable to deploy emergency aid/response

Prepare explosive drones as backup plan

Deploy to substation linked to Stock Exchange to disrupt financial systems if don't pay up

- Track & monitor ransomware incidents.
- Engage respective CERT for response & recovery of critical systems.
- Monitoring & Response are two distinct & separated functions.



Privacy & Security

Ransomware: See the 14 hospitals attacked so far in 2016

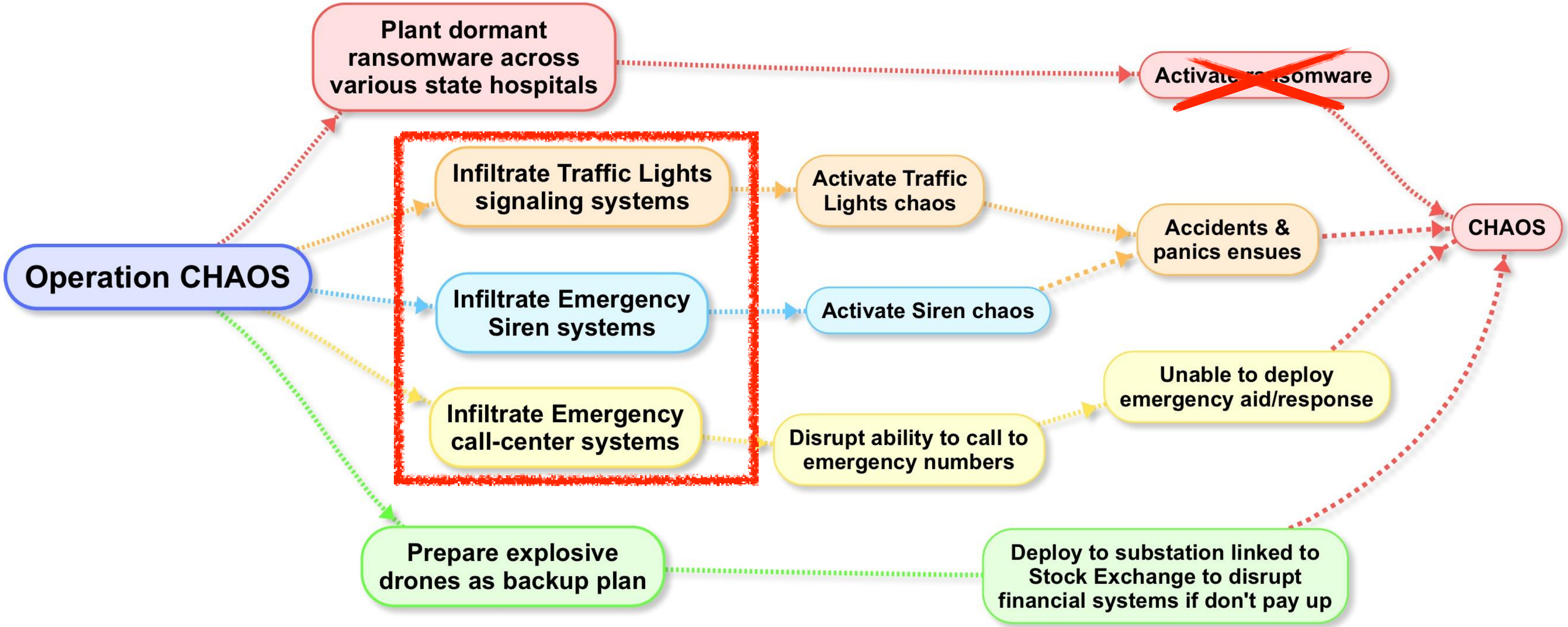
By Jessica Davis | October 05, 2016 | 12:13 PM

1 slide of 13

Ransomware attacks have been steadily increasing in the healthcare industry since the beginning of the year, and with the most recent attacks on New Jersey Spine Center, Marin Healthcare District and Urgent Care Clinic of Oxford, it doesn't look like

NATIONAL CSOC + Crisis Coordination

- Together with CERT & system owners, the **clean-up** of malware would have **change the course** of Operation CHAOS… or…
- **Let’s imagine they proceed ahead & succeed in infiltration & disruption… but don’t realise that the dormant ransomware was removed…**
- **How would the story continue with the National CSOC?**



Operation CHAOS

Plant dormant ransomware across various state hospitals

~~Activate ransomware~~

Infiltrate Traffic Lights signaling systems

Activate Traffic Lights chaos

Infiltrate Emergency Siren systems

Activate Siren chaos

Accidents & panics ensues

CHAOS

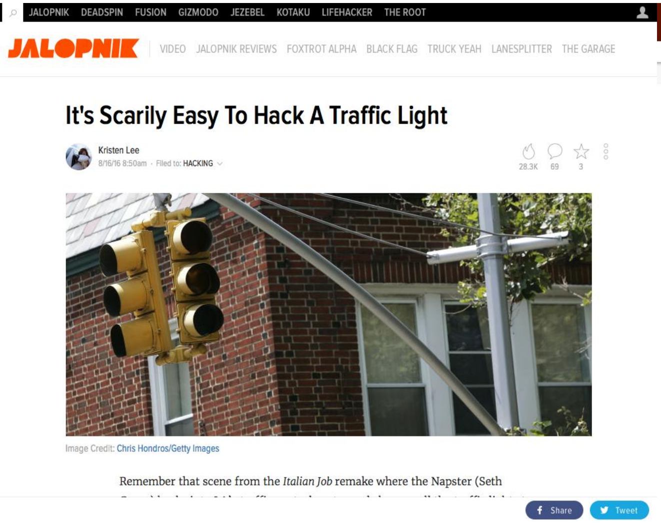
Infiltrate Emergency call-center systems

Disrupt ability to call to emergency numbers

Unable to deploy emergency aid/response

Prepare explosive drones as backup plan

Deploy to substation linked to Stock Exchange to disrupt financial systems if don't pay up

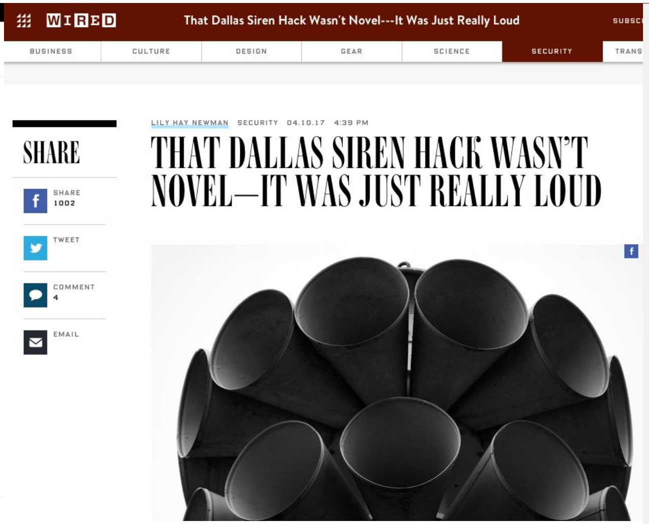


It's Scarily Easy To Hack A Traffic Light

Kristen Lee
8/16/16 8:50am · Filed to: HACKING

Image Credit: Chris Hondros/Getty Images

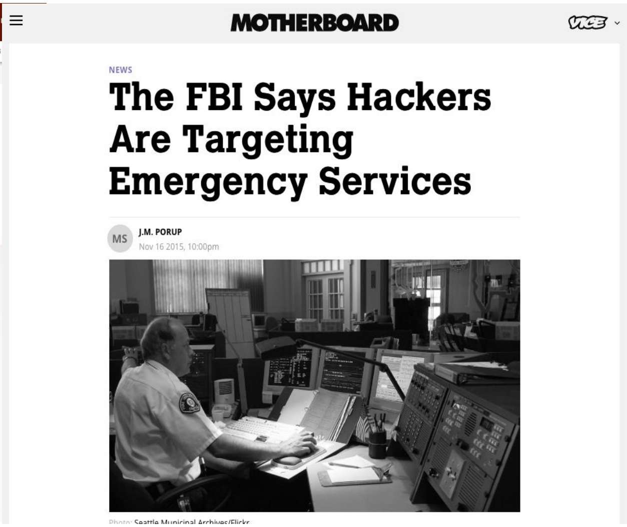
Remember that scene from the *Italian Job* remake where the Napster (Seth



That Dallas Siren Hack Wasn't Novel---It Was Just Really Loud

LILY HAY NEWMAN SECURITY 04.10.17 4:39 PM

THAT DALLAS SIREN HACK WASN'T NOVEL—IT WAS JUST REALLY LOUD

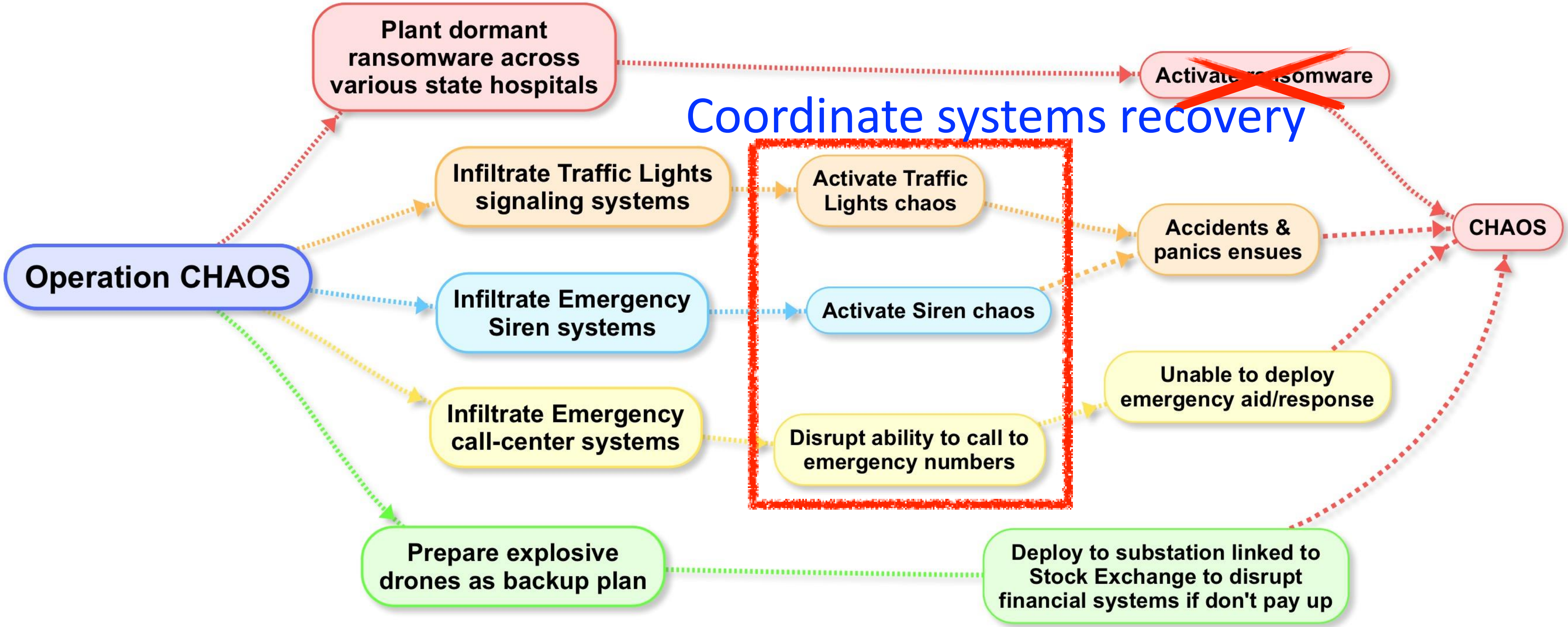


NEWS

The FBI Says Hackers Are Targeting Emergency Services

J.M. PORUP
Nov 16 2015, 10:00pm

Photo: Seattle Municipal Archives/Flickr


Plant dormant ransomware across various state hospitals

~~Activate ransomware~~

Coordinate systems recovery

Operation CHAOS

Infiltrate Traffic Lights signaling systems

Activate Traffic Lights chaos

Accidents & panics ensues

CHAOS

Infiltrate Emergency Siren systems

Activate Siren chaos

Unable to deploy emergency aid/response

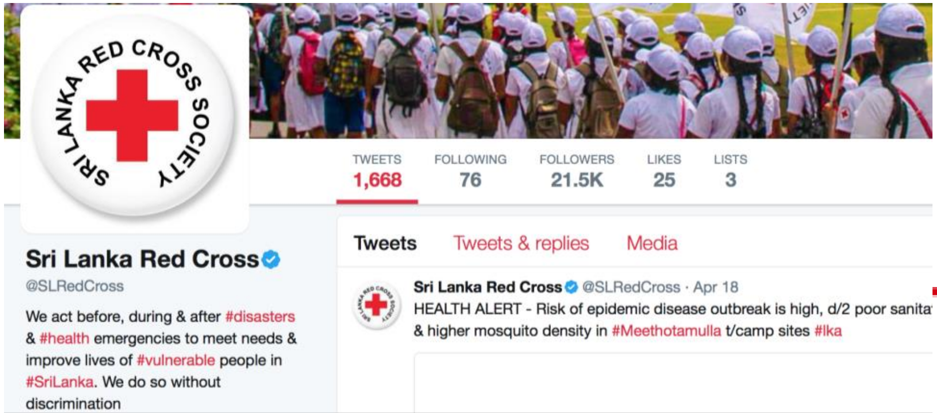
Infiltrate Emergency call-center systems

Disrupt ability to call to emergency numbers

Prepare explosive drones as backup plan

Deploy to substation linked to Stock Exchange to disrupt financial systems if don't pay up

- Official channels are down… citizens will use social media.


SRI LANKA RED CROSS SOCIETY

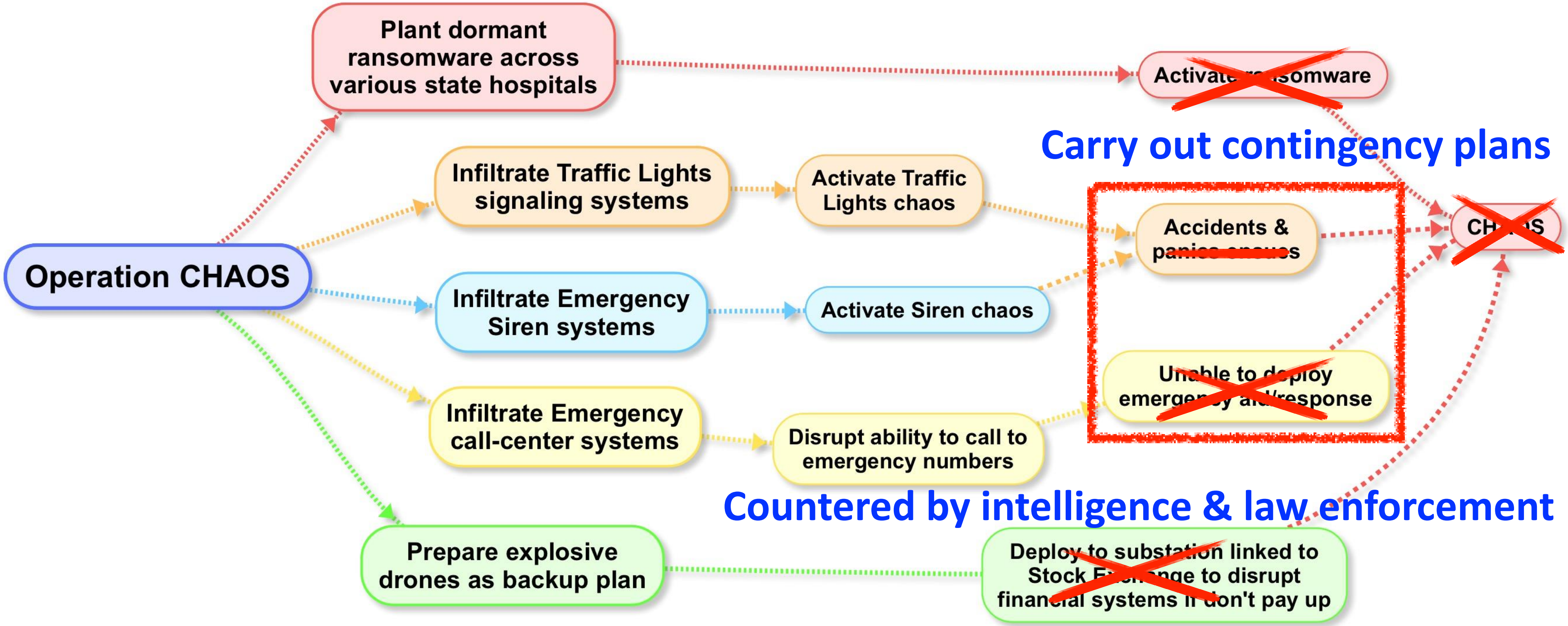
TWEETS 1,668
FOLLOWING 76
FOLLOWERS 21.5K
LIKES 25
LISTS 3

Tweets   Tweets & replies   Media

Sri Lanka Red Cross
@SLRedCross

We act before, during & after #disasters & #health emergencies to meet needs & improve lives of #vulnerable people in #SriLanka. We do so without discrimination

Sri Lanka Red Cross @SLRedCross · Apr 18
HEALTH ALERT - Risk of epidemic disease outbreak is high, d/2 poor sanita
& higher mosquito density in #Meethotamulla t/camp sites #lka



Operation CHAOS

Plant dormant ransomware across various state hospitals

~~Activate ransomware~~

Infiltrate Traffic Lights signaling systems

Activate Traffic Lights chaos

Infiltrate Emergency Siren systems

Activate Siren chaos

Infiltrate Emergency call-center systems

Disrupt ability to call to emergency numbers

Accidents & ~~panics ensues~~

~~Unable to deploy emergency aid/response~~

~~CHAOS~~

Prepare explosive drones as backup plan

~~Deploy to substation linked to Stock Exchange to disrupt financial systems if don't pay up~~

Carry out contingency plans

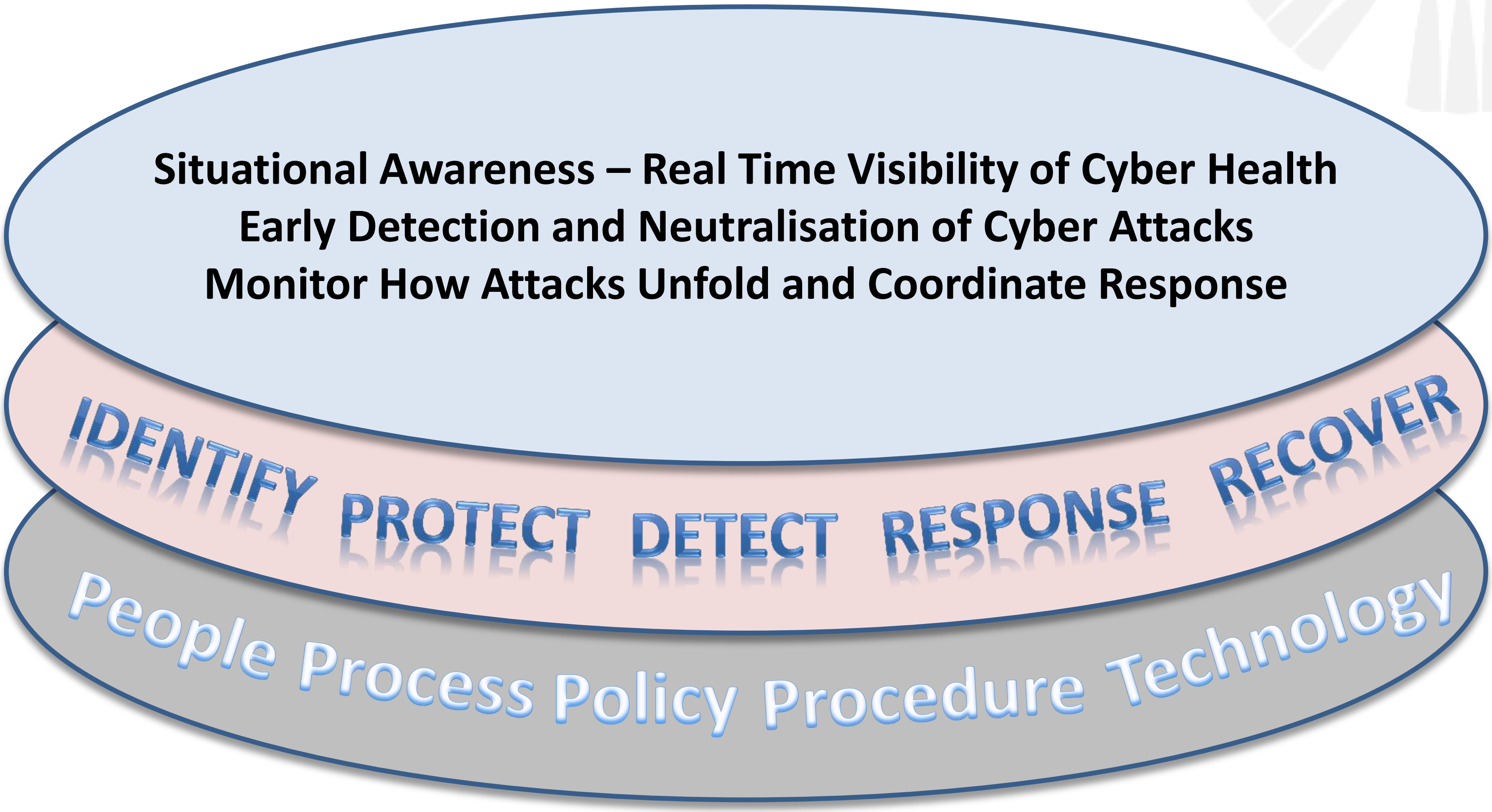
Countered by intelligence & law enforcement

- Skilled analysts @ National CSOC can extract geo-location-metadata in social media posts & photos to pin-point incidents' locations.
- Crisis coordination, Intelligence & Law enforcement agencies have right data & tools to respond & recover.

NATIONAL CSOC is Essential

- For EARLY WARNING **(Before)**.
- For SITUATIONAL AWARENESS & RESPONSE **(During)** .
- For EFFECTIVE Crisis Management **(After)** .
- **During peace-time, how the National CSOC is used should be part of National Emergency Response Planning & Exercises.**

National CSOC Mission

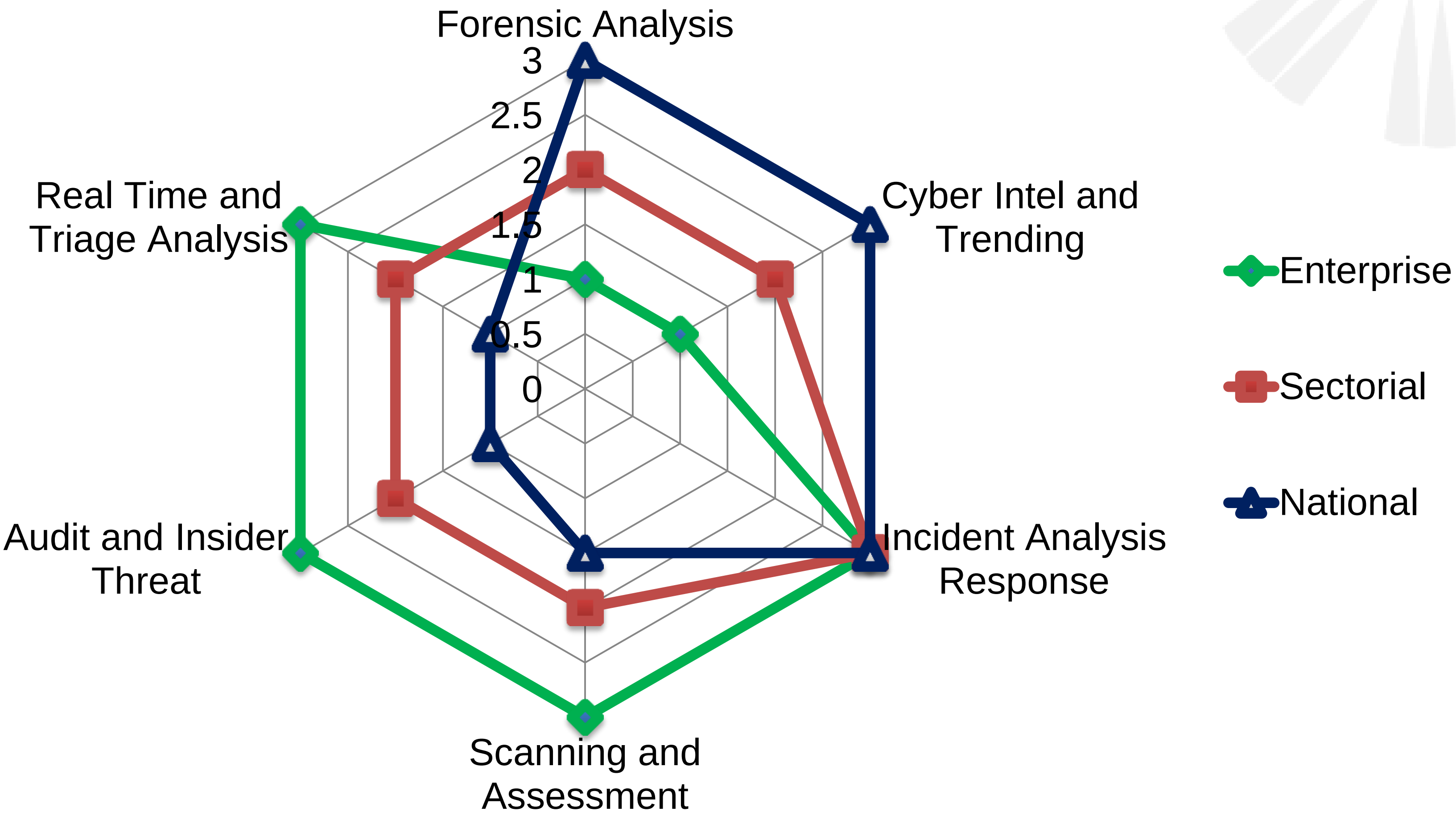


Situational Awareness – Real Time Visibility of Cyber Health
Early Detection and Neutralisation of Cyber Attacks
Monitor How Attacks Unfold and Coordinate Response

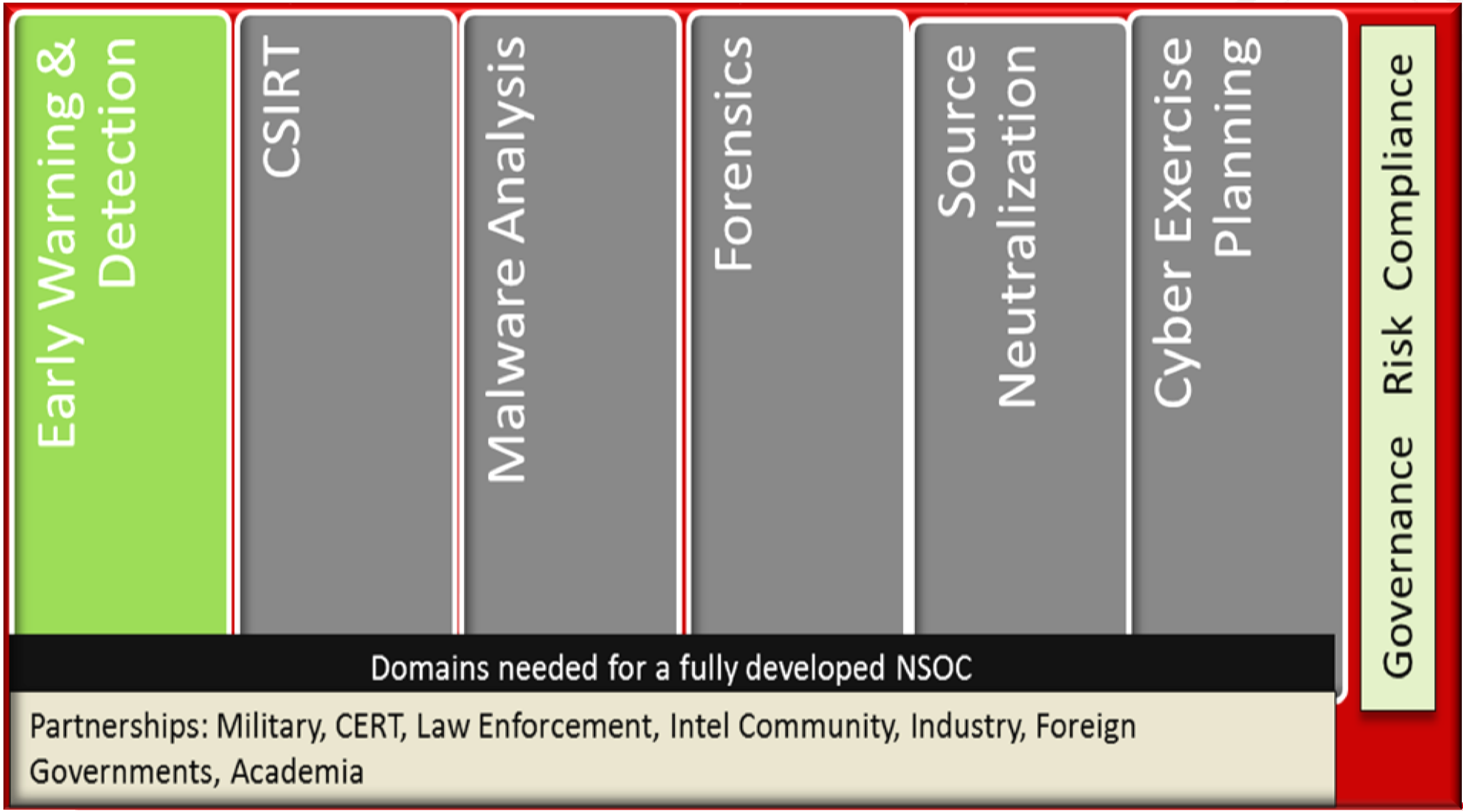
IDENTIFY PROTECT DETECT RESPONSE RECOVER

People Process Policy Procedure Technology

National, Sectorial and Enterprise SOC



NCSOC Domains and Functions



Early Warning & Detection

CSIRT

Malware Analysis

Forensics

Source Neutralization

Cyber Exercise Planning

Governance Risk Compliance

Domains needed for a fully developed NSOC

Partnerships: Military, CERT, Law Enforcement, Intel Community, Industry, Foreign Governments, Academia

ST Electronics
Info-Security
A member of ST Engineering

Thank You

ENGINEERING
WITH PASSION

Empowering thru' Innovation

I AWARD