



The Federmann Cyber Security Center – Law Program

Lunchtime gathering of cyber experts, students, professors, entrepreneurs, and government leaders.



Regulating Trust in Cyberspace: A Polycentric Model for Critical Cyber Information Sharing

WANNACRY

2017 במאי 12-14

The 'Wannacry' ransomware attack

The attack has hit more than 200,000 victims in at least 150 countries, says Europol

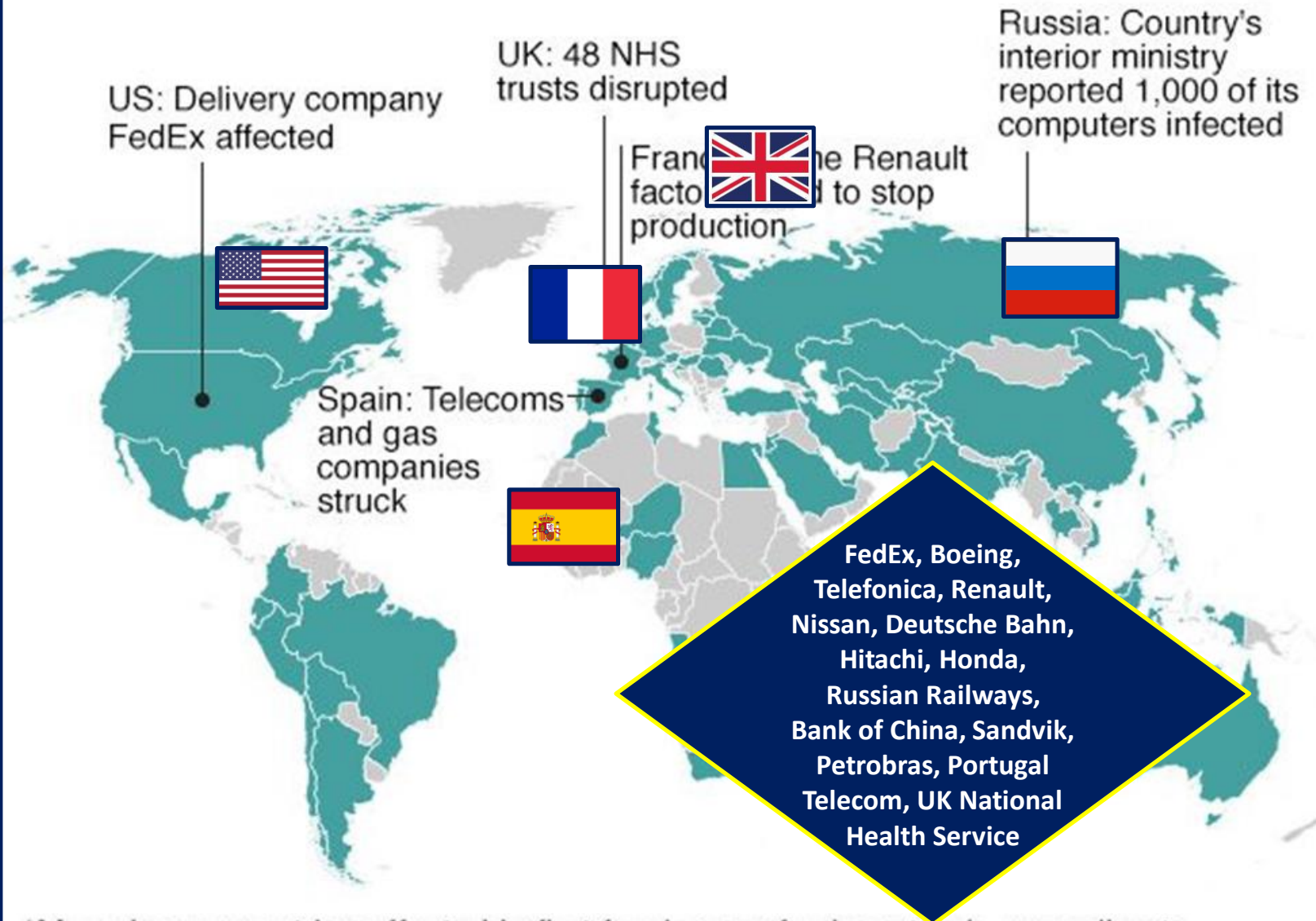


Source: Intel.malwaretech.com



© AFP

Countries hit in initial hours of cyber-attack



*Map shows countries affected in first few hours of cyber-attack, according to Kaspersky Lab research, as well as Australia, Sweden and Norway, where incidents have been reported since

שיתוף המידע שמזער את ההתפשטות של WannaCry ונזקי הפעילות העויינת

12.5 – בוקר

12.5 – צהריים

12-13.5 –
במהלך הלילה

12-13.5

13.5

Cybersecurity
Information
Sharing
Partnership
(CiSP)

משתף מידע
ראשוני עם
שותפים ב-UK

@MalwareTech
Blog משתף דרך
קהילת
האנאליסטים
המקצועיים

ארגון
ShadowServer
DHS-וה-FBI
משתפים דרך
הרשתות שלהם

שיתוף פומבי דרך
CSIRT ו-CERTs

חב' מיקרוסופט
patch מפצה

14.4 ארגון

Shadow Brokers

מצליחים לגנוב כלי חשיפה

בשם

ETERNAL BLUE

מה-

NSA

שאינו משתף מידע לגבי
הגניבה

DHS: "We are **actively sharing information** related to this event and stand ready to lend technical support and assistance as needed to our partners, both in the United States and internationally."



בלמ"ס

TLP: לבן

- 1 -

13/05/2017

י"ז באייר תשע"ז

סימוכין: ב-ס-160

אירוע "חץ וקשת" - הנחיות התמודדות עם כופרת WannaCry

(מעודכן נכון ל-14/05/2017 בשעה 11:45. השינוי בהוספת סעיפים 2,5 ו-15 בהמלצות

הטכני)

תקציר

ביום שישי ה-12 במאי זוהה גל התקפות כופרה מאסיבי כנגד עשרות אלפי מחשבים בארגונים רבים ובעשרות מדינות ברחבי העולם, ביניהם Telefonica בספרד, שירות הבריאות הלאומי בבריטניה ו-FedEx בארה"ב. התקיפה מנצלת חולשת אבטחה אשר פורסמה בהדלפות Shadow Broker במהלך חודש

מרקוס האצ'ינס @MalwareTech



shadowserver

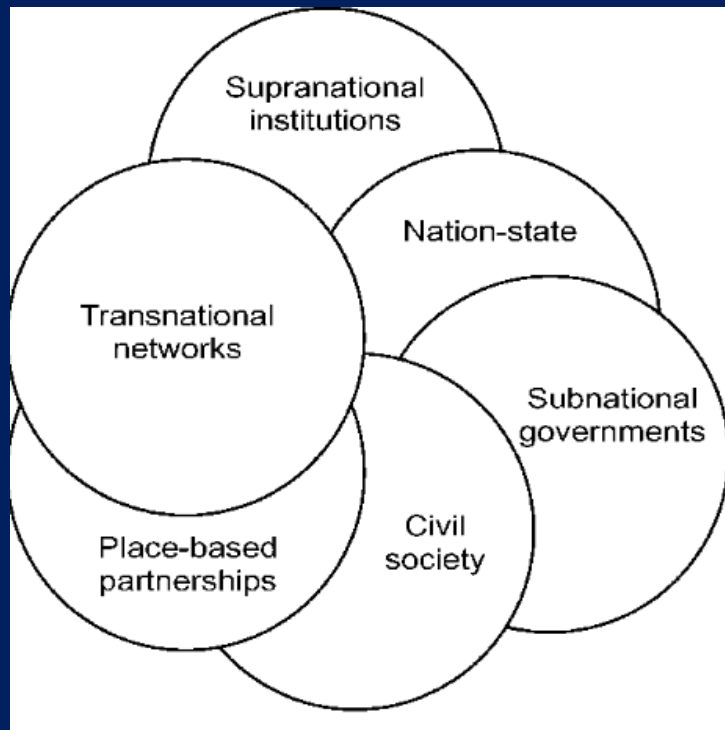
NGO



טענת הבסיס של המחקר

המודל הרגולטורי המתאים ביותר להסדרת שיתוף
מידע לזיהוי איומי סייבר ומזעור נזקים הוא **מודל**
פוליסנטרי

+ כמה תוספות



Bulkeley *et al*, 2003

Polycentricity is a regulatory approach and framework for ordering the actions **of a multiplicity of state and non-state actors** around a **common aim**, sometimes described in the literature as a "collective action problem". This approach also incorporates a multiplicity of measures (Shackelford, 2018)

הגדרת הבעיה: רוב המודלים הקיימים לש"מ לתמוך בהגנת סייבר אינם פוליצנטרים ואינם אופטימליים

1. אם מדובר בחובה סטטורית שמטילה המדינה על ארגונים פרטיים לשתף מידע סייברי (מוסדות פיננסיים)

- חששות מפני חשיפות משפטיות ב-4 מישורים

- ❖ שיתוף מידע הלאה בתוך גורמי ממשל
- ❖ הגנת מידע אישי של לקוחות, עובדים ספקים
- ❖ הגנת IP ארגוני
- ❖ סיכוני הגבלים עסקיים ברמה המגזרית

2. אם מדובר בש"מ התנדבותי (ארגון מגזרי, מדינה-תעשייה)

- חוסר תמריץ רגולטורי
- בעיית מחויבות
- free riders

1. המודלים הקיימים מתבססים על **תפיסות רג'** שמרניות

- top down, מדינה < מגזר פרטי
- במיוחד לגבי תשתיות קריטיות באמצעות רגולציה בעלת אופי בטחוני (US DHS, ישראל ב/84, 8ב5)

2. שיתוף המידע הרבה פעמים **חד-כיווני ואינו מאפשר מינוף המידע הקיים** בקרב כל בעלי העניין הרלוונטיים

- המגזר פרטי מעביר מידע << גורמי מדינה
- **עמימות** לגבי שימוש המידע שנאסף מצד המדינה



בעיית אמון

3. כלים ואמצעים **לא מתאימים**

- חשופים לפריצות (NSA)
- לא משקפים **התפתחויות טכנולוגיות** בצד התוקפים ובכלל

מצד שני, שיתוף מידע הוא קריטי להגנת סייבר

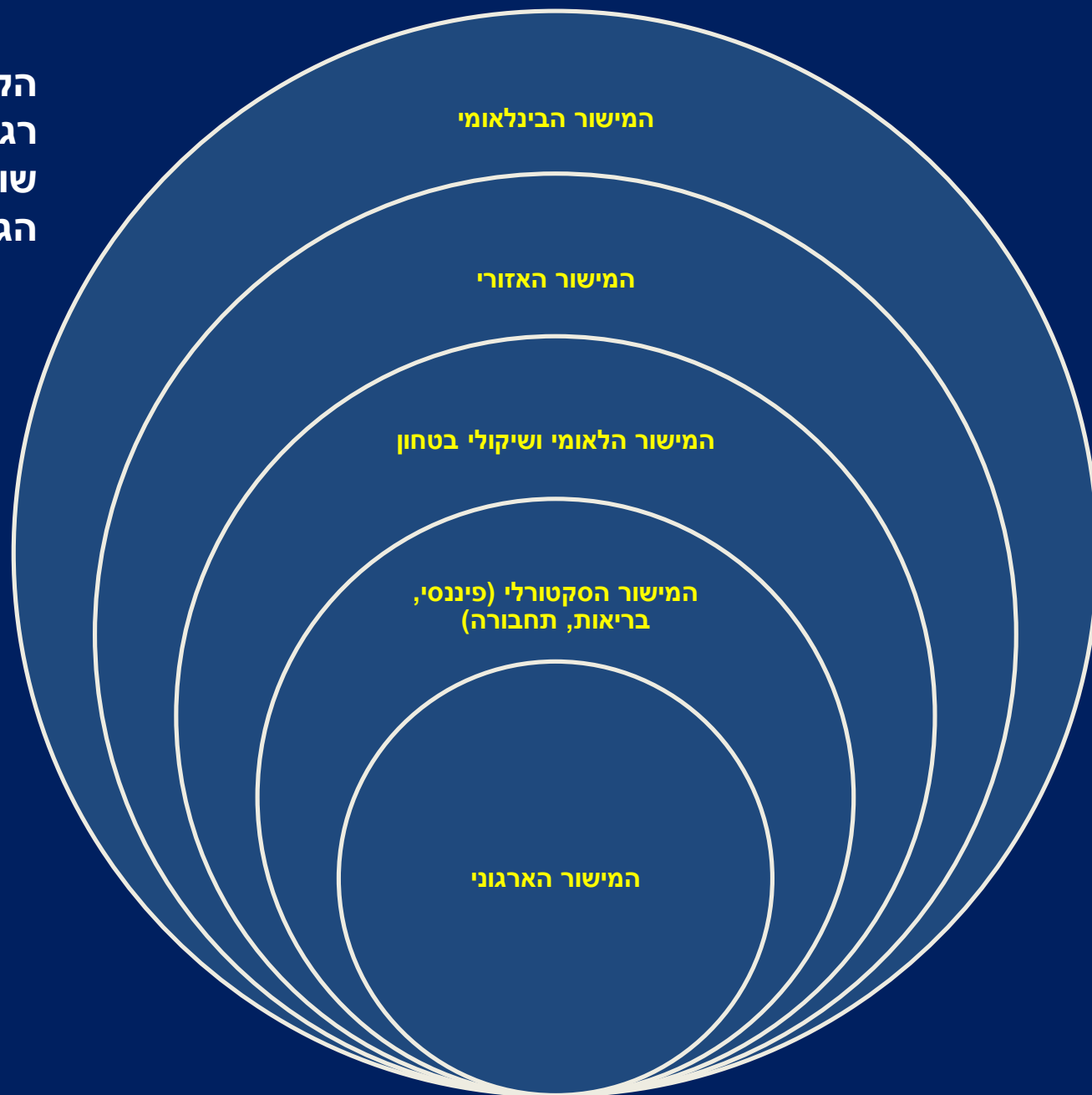
- ש"מ מגשר על האסימטריות במידע (informational asymmetry) בין התוקף לבין הארגונים המותקפים

- מאפשר זיהוי יחסית מהיר של חשיפות ומזעור נזקים
— Wannacry

- ברמה האסטרטגית, גיבוש best practices - "גאות גאות מעלה את כל הסירות"



הקשרים
רגולטוריים
שונים של
הגנת סייבר



האיומים והעלויות - מחייבים מענה רגולטורי



~טריליון \$
לשנה

WEF GLOBAL RISKS
REPORT 2019 - The
Global Risks
Landscape

למה זה מעניין מבחינה משפטית?

האתגרים המשפטיים-רגולטוריים: 4 מחסומים לש"מ

1. חוסר שקיפות

- מידע שעובר לגורמי ממשל עלול לעבור בין רשויות, ללא אפשרות מבחץ לעקוב אחרי השימושים
- חשש מפני חשיפת הארגון המשתף מהעברת "מידע מפליל" לגורמי אכיפה אחרים

2. שיתוף במידע אישי אינו מוגן ברמה מספקת

- לקוחות, עובדים, ספקים
- חשיפת הגורם המשתף לסנקיות מרגולטור אחר / תביעות, תובענות ייצוגיות

האתגרים המשפטיים-רגולטוריים: 4 מחסומים לש"מ (ב')

3. **שיתוף ב- IP** של הארגון אינו מוגן ברמה מספקת

- בין ארגונים: חשיפת יכולות, טכנולוגיות, תהליכים
- חשיפה לתביעות מצד בעלי מניות

4. השלכות בהקשר של **דיני תחרות והגבלים עסקיים**

- שיתוף ידע בין ארגונים באותו המגזר

בפרספקטיבה רחבה יותר:
הפרויקט הנורמטיבי הכללי של המשפט
הבינלאומי במרחב הסייבר
בין נורמות מחייבות ו-CBMs



(3) שאלות לדין

(2) המודל
הפוליסנטרי

(1) הגדרות
ודוגמאות של
רגולציה
לש"מ

By exchanging cyber threat information within a sharing community, organizations can **leverage the collective knowledge, experience, and capabilities** of that sharing community to gain **a more complete understanding of the threats** the organization may face. Using this knowledge, *an organization can make threat-informed decisions regarding defensive capabilities, threat detection techniques, and mitigation strategies.* By correlating and analyzing cyber threat information from multiple sources, an organization can also **enrich existing information and make it more actionable.**

טיפול
רגולטורי ב-
informational
assymetries

NIST, Guide to Cyber Threat Information Sharing, 2016

באזה מידע משתפים ומתי?



Info Sharing Requires Trust


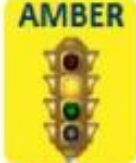


TLP – Traffic Light Protocol

What is TLP?

A set of designations to ensure that sensitive information is shared with the correct audience and that the recipient (s) understand if and how the information can be disseminated.

Who Uses TLP?

US-CERT, public and private sector organizations within: US, Australia, Canada, Finland, France, Germany, Hungary, Italy, Japan, Netherlands, New Zealand, Norway, Sweden, Switzerland and the United Kingdom.

Color	How may it be shared?
	Recipients may not share TLP: RED information with any parties outside of the specific exchange, meeting, or conversation in which it is originally disclosed.
	Recipients may only share TLP: AMBER information with members of their own organization who need to know, and only as widely as necessary to act on that information.
	Recipients may share TLP: GREEN information with peers and partner organizations within their sector or community, but not via publicly accessible channels.
	TLP: WHITE information may be distributed without restriction, subject to copyright controls.

Source: US Cert <https://www.us-cert.gov/tlp>

Structured Threat Information Expression
(STIX), Cyber Observable Expression
(CybOX)

דוגמה 1: EU NIS Directive, 2016

Article 1

Subject matter and scope

1. This Directive lays down measures with a view to achieving a high common level of security of network and information systems within the Union so as to improve the functioning of the internal market.

2. To that end, this Directive:

- (c) ~~creates a computer security incident response teams network ('CSIRTs network') in order to contribute to the development of trust and confidence between Member States and to promote swift and effective operational cooperation;~~
- (e) lays down **obligations for Member States** to designate national competent authorities, single points of contact and CSIRTs with tasks related to the security of network and information systems.

6. This Directive is without prejudice to the actions taken by Member States to safeguard their essential State functions, in particular **to safeguard national security, including actions protecting information the disclosure of which Member States consider contrary to the essential interests of their security, and to maintain law and order, in particular to allow for the investigation, detection and prosecution of criminal offences.**

אין הגנות לגופים שמשתפים IP או מידע אישי

דוגמה 2: US Cybersecurity Information Sharing Act of 2014

113TH CONGRESS
2^D SESSION

S. 2588

To improve cybersecurity in the United States through enhanced sharing of information about cybersecurity threats, and for other purposes.

IN THE SENATE OF THE UNITED STATES

JULY 10, 2014

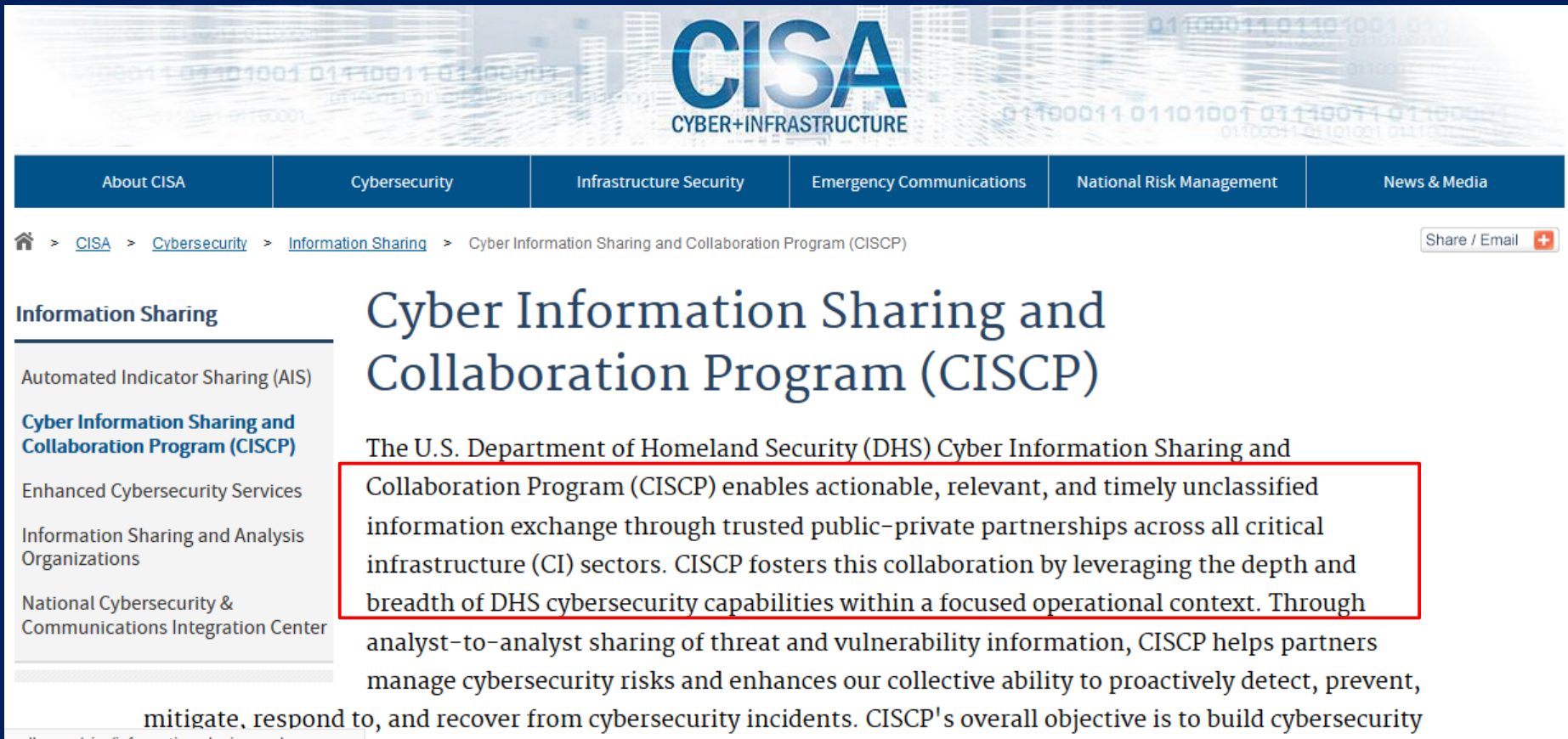
Mrs. FEINSTEIN, from the Select Committee on Intelligence, reported the following original bill; which was read twice and placed on the calendar

A BILL

To improve cybersecurity in the United States through enhanced sharing of information about cybersecurity threats, and for other purposes.

- מאפשר ש"מ עם הגנות מפני הגבלים עסקיים
- התנדבותי
- “and for other purposes”

דוגמה DHS:2



The screenshot shows the DHS CISA website. The header features the CISA logo (CYBER+INFRASTRUCTURE) and a navigation bar with links: About CISA, Cybersecurity, Infrastructure Security, Emergency Communications, National Risk Management, and News & Media. Below the navigation bar is a breadcrumb trail: Home > CISA > Cybersecurity > Information Sharing > Cyber Information Sharing and Collaboration Program (CISCP). A 'Share / Email' button is visible in the top right. The main content area has a left sidebar with links: Information Sharing, Automated Indicator Sharing (AIS), Cyber Information Sharing and Collaboration Program (CISCP), Enhanced Cybersecurity Services, Information Sharing and Analysis Organizations, and National Cybersecurity & Communications Integration Center. The main heading is 'Cyber Information Sharing and Collaboration Program (CISCP)'. The introductory text states: 'The U.S. Department of Homeland Security (DHS) Cyber Information Sharing and Collaboration Program (CISCP) enables actionable, relevant, and timely unclassified information exchange through trusted public-private partnerships across all critical infrastructure (CI) sectors. CISCP fosters this collaboration by leveraging the depth and breadth of DHS cybersecurity capabilities within a focused operational context. Through analyst-to-analyst sharing of threat and vulnerability information, CISCP helps partners manage cybersecurity risks and enhances our collective ability to proactively detect, prevent, mitigate, respond to, and recover from cybersecurity incidents. CISCP's overall objective is to build cybersecurity'.

CISA
CYBER+INFRASTRUCTURE

About CISA Cybersecurity Infrastructure Security Emergency Communications National Risk Management News & Media

Home > CISA > Cybersecurity > Information Sharing > Cyber Information Sharing and Collaboration Program (CISCP) Share / Email

Information Sharing

- Automated Indicator Sharing (AIS)
- Cyber Information Sharing and Collaboration Program (CISCP)**
- Enhanced Cybersecurity Services
- Information Sharing and Analysis Organizations
- National Cybersecurity & Communications Integration Center

Cyber Information Sharing and Collaboration Program (CISCP)

The U.S. Department of Homeland Security (DHS) Cyber Information Sharing and Collaboration Program (CISCP) enables actionable, relevant, and timely unclassified information exchange through trusted public-private partnerships across all critical infrastructure (CI) sectors. CISCP fosters this collaboration by leveraging the depth and breadth of DHS cybersecurity capabilities within a focused operational context. Through analyst-to-analyst sharing of threat and vulnerability information, CISCP helps partners manage cybersecurity risks and enhances our collective ability to proactively detect, prevent, mitigate, respond to, and recover from cybersecurity incidents. CISCP's overall objective is to build cybersecurity

דוגמה 3: בנק ישראל נב"ת 361 ממרץ 2016: "ניהול הגנת הסייבר"

שיתוף מידע ומודיעין

64. התאגיד הבנקאי יאסוף וינתח מידע רלבנטי, ממקורות פנימיים וחיצוניים, לצורך יצירת תפיסה כוללת ועדכנית של תמונת איום הסייבר והחשיפה של התאגיד הבנקאי למולו, כבסיס לקבלת החלטות מושכלת, תעדוף של דרכי פעולה, וקיום הגנה אפקטיבית בזמן אמת.

66. התאגיד הבנקאי ישתף מידע שעשוי לסייע לתאגידים בנקאיים אחרים בהתמודדות מול איומי סייבר.

67. איסוף ושיתוף המידע יתבצע בהתאם להנחיות המפקח ובכפוף לדין.

FC3



היעדים המרכזיים של מרכז סייבר ורציפות פיננסית

- חיזוק החוסן הפיננסי של ישראל
- הקמת תשתית לשיתופי מידע ופעולה
- גיבוש הערכת מצב למקבלי ההחלטות

המרכז כולל צוות מקצועי לשיתוף מידע ולניהול אירועי אבטחת מידע, סייבר ורציפות תפקודית ומשרת את המגזר הפיננסי במדינת ישראל וביניהם: משרד האוצר, בנק ישראל, גופי הפיקוח המגזריים והגופים הפיננסיים המפוקחים: בנקים, חברות ביטוח, גופי השקעות והבורסה לניירות ערך.

תזכיר חוק הגנת הסייבר ומערך הסייבר הלאומי, התשע"ח-2018

פעילות מותרת 65. (א) לא יראו שיתוף של מידע שנאסף בארגון, עם ארגון נוסף או יותר, או עם מערך הסייבר הלאומי כפגיעה בפרטיות לפי חוק הגנת הפרטיות, אם מתקיימים כל אלה:

לצרכי הגנת הסייבר

- (1) המידע הוא מידע בעל ערך אבטחתי;
- (2) הארגון מסר פרטים על הפעילות, על מטרותיה, ועל השימוש במידע במסגרתה לעובדיו ולקוחותיו;
- (3) השימוש במידע הוא למטרת הגנת הסייבר.

שיתוף מידע

66.

לצורכי הגנה –

פעולה מותרת

לא יראו שיתוף מידע בעל ערך אבטחתי בין שני ארגונים או יותר למטרת הגנת

סייבר, כהפרה של הוראות חוק ההגבלים העסקיים, התשמ"ח-1988,¹⁴ בתנאי

שיתקיימו כל אלה:

(1) המידע אינו כולל נתונים על לקוחות, ספקים, כמויות או מחירים של

הארגונים;

(2) המידע אינו כולל מידע על איכות מוצר או שירות המסופק על ידי אחד

הארגונים.

מערך הסייבר הלאומי



סייבר ישראל
מערך הסייבר הלאומי

119 

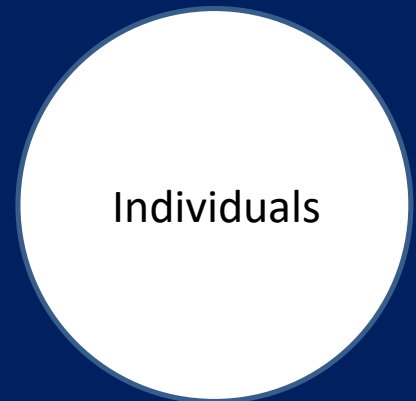
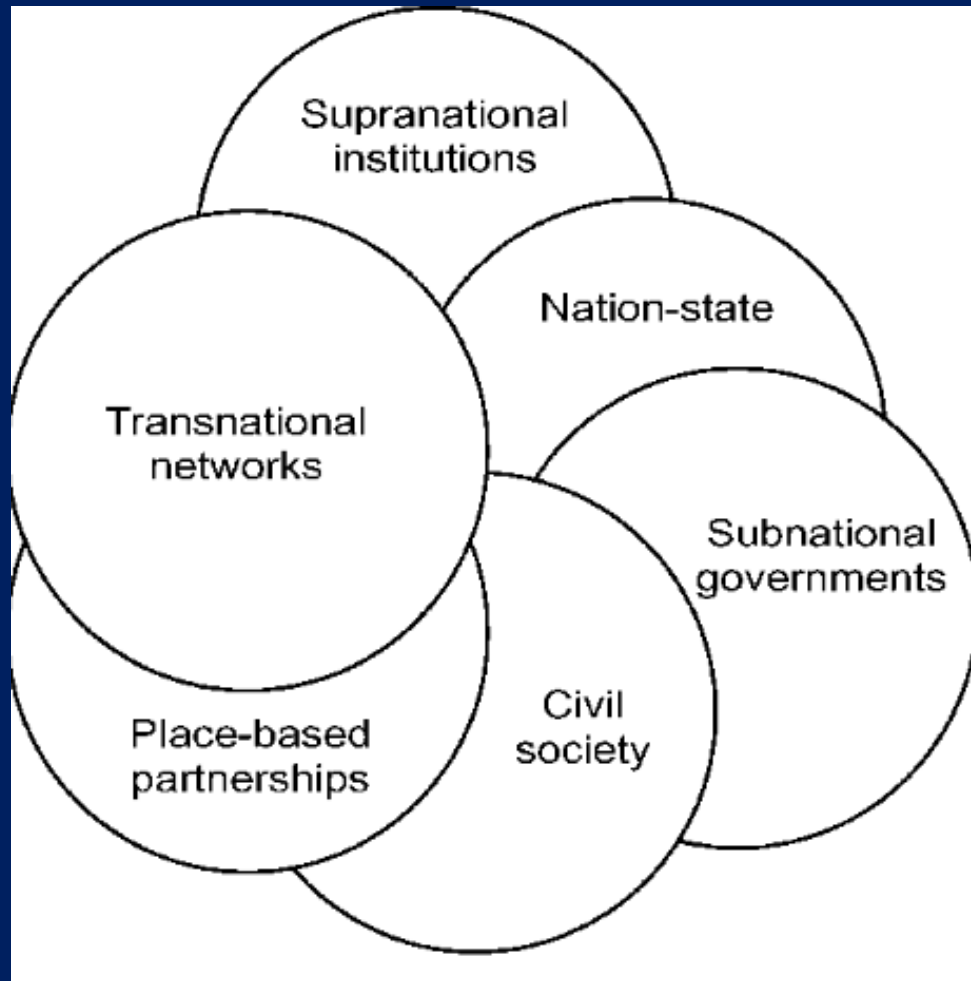
המרכז המבצעי
לניהול אירועי סייבר

וידאו | נושאים | חדשות | אודות | צדוקשר | פר

המגמה: פלטפורמות ממשל-סקטור פרטי לשיתוף מידע



(2) המודל הפוליסנטרי להתמודדות עם האתגרים ובניית האמון הנדרש



Bulkeley *et al*, 2003

אלינור אוסטרום ותפיסת הפוליצנטריות

- אוסטרום זכתה בפרס נובל ב-2009 על עבודתה בנוגע לפוליצנטריות כדרך הטובה ביותר לנהל ממשאבים משותפים (commons) כגון יערות, דייג, שטחי מרעה, שדות נפט ועוד מרחבים משותפים.



- מדובר בקשר בין אמון והדדיות (trust and reciprocity) והדרכים האופטימליים להסדיר אותם

Julia Black, 2008

“By regulation is meant sustained and focused attempts to change the behavior of others in order to address a **collective problem** or attain an identified end or ends, usually through a combination of rules or norms and some means for their implementation and enforcement, which can be legal or non-legal.

The regulatory functions can be exercised primarily by one actor or dispersed between a number of actors. The greater the dispersal and fragmentation of actors in the performance of regulation, including the definition of the problem/goals, the greater the **polycentricity** of the regime.”

התפיסה פותרת מספר סוגיות ש"מ

- הצורך לכלול **כמה שיותר "סנסורים"** לפעילות עוינת במרחב
- **יישום כלים** ואמצעים מגוונים, חדשנים ורלוונטיים
- **פיקוח (oversight) רחב יותר** על שמירת זכויותיהם של הגורמים הלא-מדינתיים

מרקוס האצ'ינס @MalwareTech



shadowserver

NGO



ש"מ לפי המודל הרגולטורי המוצע

- במישור התפעולי

- פלטפורמה לשיתוף מידע שהוא מאובטח ברמה גבוהה, המאפשר שיתוף מהיר, מדויק ורלוונטי
- יישום אמצעים טכנולוגיים חדשנים / מעודכנים

- במישור הרגולטורי – משפטי

- ריבוי משתתפים

- מדינה
- מגזר פרטי (יתכן שיתקיים על בסיס מגזרי, עם אפשרות ל-scaling up)
- עמותות, NGOs, קבוצות אחרות
- אקדמיה
- יחידים (האקרים כשרים, ציבור)

- הגנות מפני חשיפות משפטיות סובסטנטיביות בקרב משתתפים

- מידע אישי
- IP
- הגבלים עסקיים



(3) שאלות לדין

(2) המודל
הפוליסנטרי

(1) הגדרות
ודוגמאות של
רגולציה
לש"מ

(3) שאלות לדיון

1. תובנות לגבי **תמריצים** רגולטוריים לשיתוף מידע בתחומים אחרים

- איכות הסביבה, הלבנת הון, מערכות בריאות
- עלויות (הכללת ש"מ כדרישה ביטוחית)

2. מחשבות על **פוליצנטריות** כאסטרטגיה רגולטורית בכלל

- התאמה למרחב הסייבר

3. האם רצוי / אשפרי **לכלול גורמי בטחון** בש"מ

- באופן מסורתי – אינם משתפים
- במרחב הסייבר, נחוץ בעיניי

תודה רבה – שאלות או הערות?


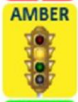


Info Sharing Requires Trust **TLP – Traffic Light Protocol**

What is TLP?

A set of designations to ensure that sensitive information is shared with the correct audience and that the recipient (s) understand if and how the information can be disseminated.

Who Uses TLP?

US-CERT, public and private sector organizations within: US, Australia, Canada, Finland, France, Germany, Hungary, Italy, Japan, Netherlands, New Zealand, Norway, Sweden, Switzerland and the United Kingdom.

Color	How may it be shared?
 RED	Recipients may not share TLP: RED information with any parties outside of the specific exchange, meeting, or conversation in which it is originally disclosed.
 AMBER	Recipients may only share TLP: AMBER information with members of their own organization who need to know, and only as widely as necessary to act on that information.
 GREEN	Recipients may share TLP: GREEN information with peers and partner organizations within their sector or community, but not via publicly accessible channels.
 WHITE	TLP: WHITE information may be distributed without restriction, subject to copyright controls.

EXTRAS



דוגמה 3: SWIFT ISAC PORTAL ToU

The SWIFT ISAC portal (the “Portal”) is a dedicated part of swift.com through which SWIFT shares information related to security threats potentially impacting our customers.

SWIFT has created the Portal for use by SWIFT users and customers. In limited instances, SWIFT may determine that it is appropriate to grant access to the Portal to business firms and other entities (always excluding natural persons) that are not SWIFT users or customers (such firms and entities are collectively referred to as “Third Parties”). The decision to grant or deny such access is solely within SWIFT’s discretion. SWIFT reserves the right to terminate any Third Party’s access to the Portal for any reason SWIFT deems appropriate.

When used in these Terms of Use, “information” means information of any nature or in any form communicated through the Portal, including, but not limited to, indicators of compromise, information about modus operandi, knowledge based tips, reports, incident reports, bulletins and the like.

"הגנת סייבר" – תזכיר, סעיף 1

...מכלול הפעולות הנדרשות למניעה, להתמודדות
ולטיפול בתקיפת סייבר או איום סייבר, לצמצום
השפעתם והנזק הנגרם מהם, במהלכם
ולאחריהם, ובכלל זה פעולות אבטחת מידע;