Security Wars
-episode 0-
Tallinn Report

株式会社ITリサーチ・アート
高橋郁夫

なぜ、タリンにいったのか
-謝辞-

- 財団法人セコム科学技術振興財団　平成20年度助成「電子証跡の追跡可能性確保による犯罪抑止と匿名性確保によるプライバシー保護の両立を目指すサイバー社会の制度および情報システム」の研究の一環である

SECOM

サイバー空間防衛隊を新設＝11年度発足目指す－防衛省

- 「防衛省は21日、同省や自衛隊へのサイバー攻撃に専門的に対処する「サイバー空間防衛隊」（仮称）を新設する方針を決めた」
  - (1)最新のコンピューターウイルス情報などの収集や対処方法の研究
  - (2)防衛省・自衛隊の指揮・通信システムの監視や防護
  - (3)専門知識を持つ要員の育成－
- ニュースを正確に読んでみましょう
  - 「防衛省や自衛隊への攻撃」
  - 「防衛省・自衛隊の指揮・通信システム」

タリンってどこですか

- エストニアの首都

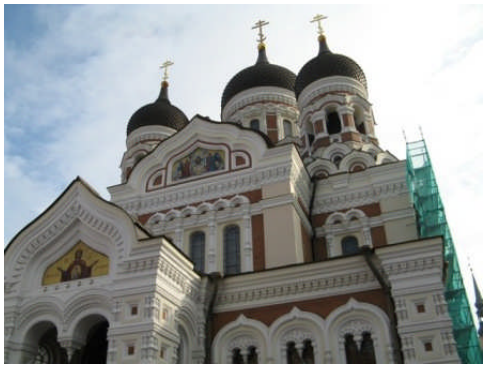
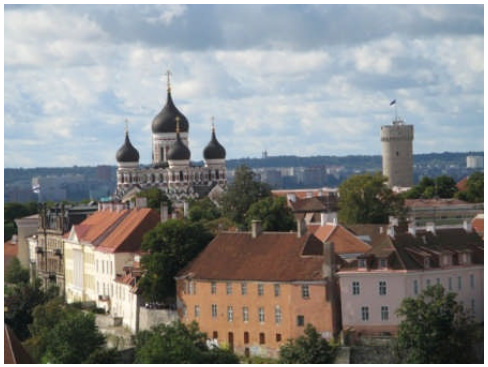
- タリンの二面性
  - 中世さながらの町
  - ハイテク進化の町

会議の主催者とテーマ

- Cooperative Cyber Defence Centre of Excellence
- NATO のResearch section
  - NATO's cyber defence capability
  - to provide insight, subject matter expertise, and assistance to NATO on various aspects of cyber defence.
- "International Cyber Conflict Legal and Policy Conference"

Old town in Tallinn



“International Cyber Conflict Legal and Policy Conference”

- “Cyber Conflict”
  - Legal and Policy
- 「サイバー戦争」とサイバー紛争
  - 「サイバー戦争の幕開け」
    - ナリタシナィジャーナルという情報誌
    - サウンドハウス(情報漏えいに直面)
- CWFI
  - LinkedInのGroup

Day0 “Boot Camp”

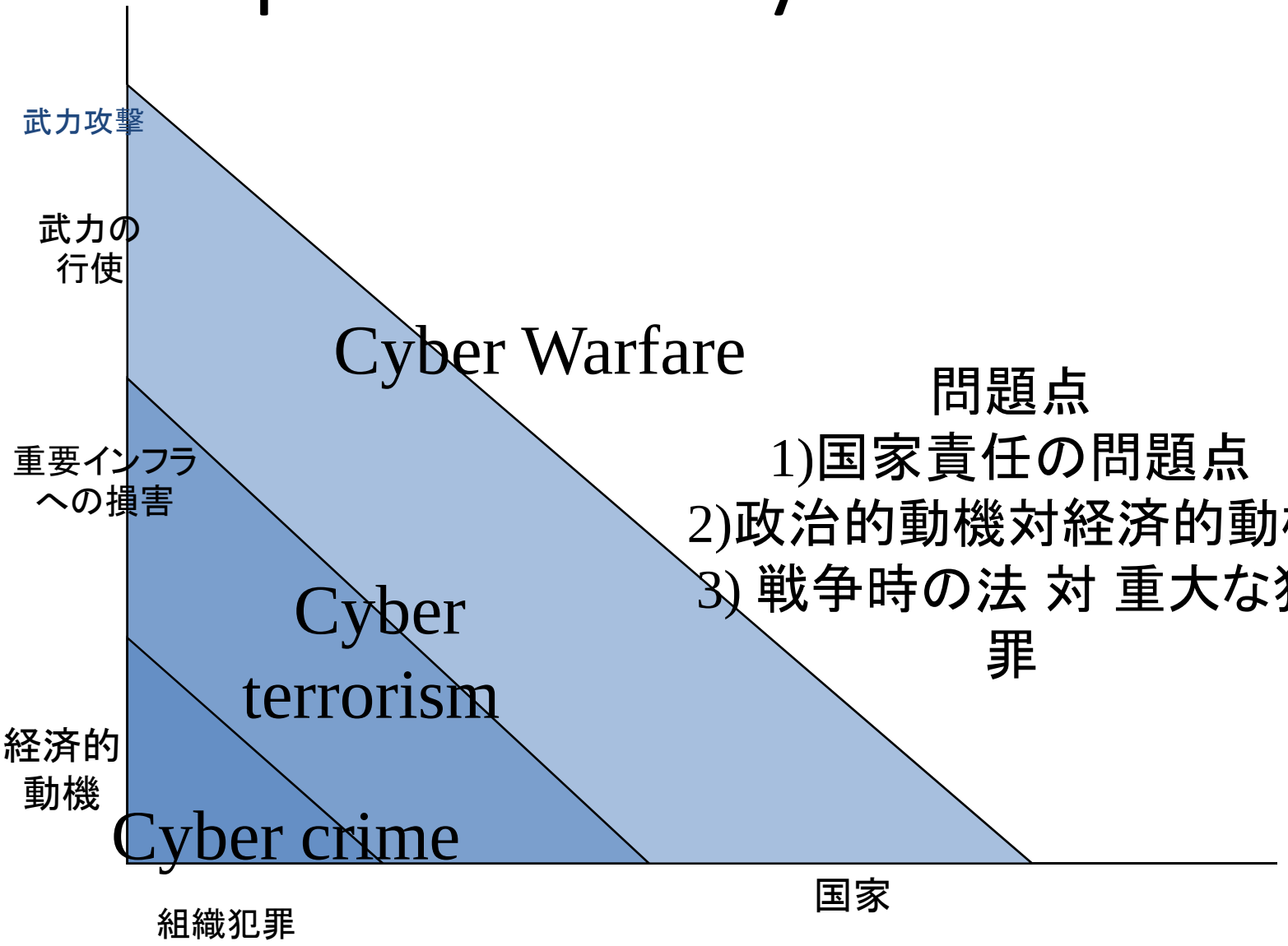
- 09:00 Lecture 1 – Frameworks for International Cyber Security (Eneken Tikk, CCD COE)
- 9:20- “Cyber Attacks and Law of Armed Conflict” (Thomas C Wingfield)
- 11:25 “Criminal Law and International Criminal Cooperation” (Markko Künnapu, Estonian Ministry of Justice)
- 12:20 “ Critical Information Infrastructure Protection Law” (Maeve Dion-Geroge Mason University)

Day0 “Boot Camp”-cont.

- 14:00 Cyber Law in the US (Dan Ryan)
- 15:15 EU Information Society Legal framework (Eneken Tikk, CCD)

visiting bronze soldier

Spectrum of Cyber Attack



問題点
1)国家責任の問題点
2)政治的動機対経済的動機
3) 戦争時の法 対 重大な犯罪

攻撃の分布と概念の限界

サイバー戦争の論点

- 法的な意味での戦争
  - 「国家の戦闘力の行使」
- ユス・アド・ベルム（Jus ad bellum）
  - 戦争を開始することの正当性の問題
- ユス・イン・ベロ（Jus in bello）
  - 戦争時の法

Jus ad bellum

- 国際連合憲章のパラダイム
- 伝統的概念の限界
  - 属性
  - 国家責任の法理
  - サイバー戦争の多義性
- 国内法との連携
  - 行政組織法
  - 刑法
- 証明の程度と判断規範

国際連合憲章のパラダイム

- 平和時（同３９条）
  - 法執行に関する論点
  - 愛国的ハッキングの合法性
- 武力の行使（同２条４項－use of force）
  - 武力の概念(force v. attack)
  - 判断手法
    - 量的(結果)判断か質的(手法)判断か-シュミットアナリシス
  - 対応手法
    - 外交・インテリジェンス・経済的制裁・武力行使
- 武力攻撃の発生（同５１条－an armed attack occurs）
- 武力による反撃（同５１条－exercise of this right of self-defense）

シュミット・アナリリシス

- Severity(被害甚大さ)
- Immediacy(緊急性)
- Directness(直接性)
- Invasiveness(侵略性)
- Measurability(計測性)
- Presumptive Legitimacy(合法性の推定)
- Responsibility(責任)

パラダイムの限界問題

- サイバー戦争の多義性
  - 物理的力・領土の意味
- 属性
  - 国家行為と愛国的暴徒
    - 伝統的な国家の指示というものがない場合でも、国家の不作為として「国家帰属」を考えるべきなのではないか
      - テロ支援国家の責任問題の認識と同一
  - 国家帰属と行為者の責任限定
    - 国家帰属とされる場合には、国際刑法上の責任をまぬがれることになるのが原則
      - 愛国的暴徒は？

国内法との連携

- 行政組織法
  - サイバー戦争についての防衛の責任は、DOD（国防省）、一方、それ以外は、その他のDHS（国土安全保安省）になる
  - 米国においても、相互の関連・情報相互の連絡に問題があり、非効率なのではないか
- (国際)刑事法
  - 刑事法の適用範囲ではない
  - 愛国的暴徒・愛国的ハッキング
  - ボットネット武装解除

Jus in bello

- **慣習法原則（Customary principle）**
  - 一般的に、ユス・イン・ベロにおける原則としては、４つのものがあげられている。
    - 「区別（無差別攻撃の禁止）」
    - 「必要性」
    - 「比例原則」
    - 「シビラリ(背信行為の禁止)」
- 中立性（Neutrality）
    - 中立義務を交戦国にたいして負う
    - 黙認、避止および防止の3種の義務

*Jus in Bello*と刑事法の交錯

- 国内刑事法が国外事案にどれだけ対応しうるのか
  - サイバーインテリジェンスの位置づけ
    - アメリカにおける『USパーソン』の意義
  - 国外通信利益の国内法的保護
    - 愛国的ハッキング
    - ボットネット武装解除
- *Jus in Bello*による適法化
  - 敵対行為(hostilities)の法的効果
  - 背信的行為と軍事的虚偽(おとりなど)の区別

LAC(戦争法)の限界
-防衛活動等の問題-

- LACと非対象戦争
  - 防衛手法の問題
    - ISPのSFUとしての役割
  - 攻撃手法の合理性

- インテリジェンス法理・監視法理との関係
  - 情報共有とプライバシーとの衝突(スウェーデンの判決)
  - わが国におけるインテリジェンス法理の未発達

Day 1 Sep.9.
“Estonian Experience”

- 9.00 Session Zero: Setting the Stage
  - Welcoming Remarks by Col Ilmar Tamm (CCD COE)
- 9.10 Keynote Address by H.E. Toomas Hendrik Ilves, President of the Republic of Estonia(ネットワークで視聴可能)
- 10.00 Keynote Address by M Gen Glynne Hines, Director NATO HQC3S
- 10.20 Frameworks for International Cyber Security: Underlying Concepts for the Conference, by Ms. Eneken Tikk, CCD COE

Day 1 “Estonian Experience”-cont.

- 11.15 Session 1: Country Reports on Cyber Security Strategy
    - Moderator: Mr. Kenneth Geers, CCDCoE
  - “Estonian Cyber Security Strategy after Lessons from 2007” National Response
    - By Ms. Heli Tiirmaa-Klaar, Ministry of Defense
  - “Sweden’s Approach to National Cyber Security”
    - By Mr. Per Oscarson, Swedish Civil Contingencies Agency
  - “Cyber Security Strategy of the United Kingdom”
    - Wg Cdr Adrian Frost
  - Q&A :Sweden の判決は、IP address = PIIといっているよという質問

Day 1 “Estonian Experience”-cont.

- Session 2: Autopsy of a Cyber Conflict
  - Moderator: Ms. Maeve L. Dion, George Mason University Center for Infrastructure Protection
  - **Lawyer’s Look at a Cyber Incident**
    - **By Prof. Daniel Ryan, USA, National Defense University, Information Resources Management Center**
  - **Cyber Conflict in Bits and Bytes**
    - **By Dr. Bret Michael, USA, Naval Postgraduate School**
  - **Industrial Control Systems Perspective**
    - **By Mr. Joe Weiss, USA, Industry Expert on Control Systems**

具体的な事案

- （１）韓国・米国に対する大規模なD-Dos攻撃
  - 20009年7月
- （２）グルジアに対するサイバー攻撃
  - 2008年8月
- （３）エストニアに対するサイバー攻撃
  - 2007年4月末

グルジアに対するサイバー攻撃-1

- 政治的状況
  - 1991年のグルジア・オセチア紛争の際に事実上独立
  - 国際的には、グルジアの一部
  - 現在でも、国連の多数は、領土的には、一部であると認識
  - 1991年のグルジア・オセチア紛争
  - 1992年には、欧州安全保障機構（OSCE）のもと、平和維持軍（ロシア、グルジア、オセチアからなる）が組織
  - グルジアとロシアの援助する分離主義者との間での緊張は、高まっていった。

- グルジアのIT化状況
  - 100名あたりのインターネットユーザは、7名（エストニアは57）
  - 近時は、ブロードバング化-着実に利用者が増加
  - 地理的に、トルコ、アルメニア、アゼルバイジャン、ロシアの「ランドルーター」を利用
  - グルジアの国際への接続状況は、約半分程度
  - 309のグルジアのプレフィックスは、トルコとアゼルバイジャン（ロシア経由）によってルーティング
  - グルジアと西ヨーロッパとのコネクションは、当時、設置目前
  - サービスプロバイダは、コーカサス・オンラインやコーカサス・ネットワーク・ツビリシが市場の90パーセン

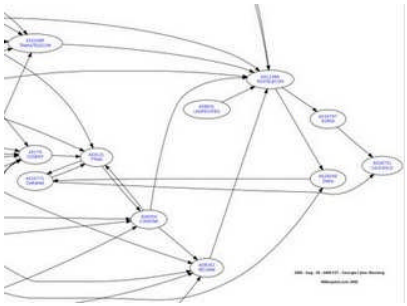
グルジアに対するサイバー攻撃-2

- 2008年8月7日
  - 分離主義者の挑発
  - グルジア軍-攻撃開始
- 翌日-ロシア軍
  - 「海外におけるロシア人の保護」の国家的義務
  - 南オセチアで、その後、平和維持強制の範囲を超えて
- 8月9日
  - ミヘイル・サーカシヴィリ・グルジア大統領、戦争状態にあると宣言した。
- 8月8日、グルジアの政府サイトに対してサイバー攻撃が開始され、
- 8月12日の停戦協定によって終了
- サイバー攻撃は、8月いっぱい継続

- 公共機関のウェブサイトの書き換え
- DDoS攻撃
- 指令および悪意あるソフトウエアの配布など
- グルジアの政治家の電子メールアドレスのリストの配布
  - スパムや標的型攻撃など

グルジア攻撃の影響と攻撃者の正体

- 重要な政府のウェブサイトにたいするDoSおよびDDoS攻撃-重要な意義
- 国際社会に対して情報を発信し、住民に対して情報を伝達する必要
- 国際社会からの支持
- 国民の士気にも影響
- グルジア国立銀行は、電子取引の提供を10日間、停止した。



- ロシア語のブログ、会議室、ウエブサイト
- バッチスクリプト（war.batというファイル名もあった）を配布
- ピン・フラッド攻撃をするかという指示
- SQLインジェクションに対して脆弱であるサイトの情報(stopgeorgia.ru など)
- ロシアのRBNも関与
- ボットネットが利用
  - コントローラーは、ロシアのハーダーによってよく使われているMachBot

エストニアに対する攻撃-1

- 2007年4月26日、27日
  首都タリン
  - ロシア系住民-暴動
  - 第二次世界大戦の記念碑- 撤去・移転-エストニア政府に反対
  - 民族主義的な運動
    - 急進化

- 4月26日
  - 1000人-記念碑の場所
    - 撤去にたいして抗議
  - 抗議-暴動化
  - 100名が負傷・1名が死亡
  - 警察-1300名を逮捕
  - 被害
  - 450万ユーロと算定
- 予定より早く記念碑の撤去-4月30日。

エストニアの情報化進展度合い

- 人口-130万人
  - 人口の密集度-低
- 発展しているIT
  - インターネットバンキング-98パーセント
  - モバイルパーキングは、50パーセントを超えて
  - モバイル交通チケットも一般化
- 行政の電子化もきわめて進展
  - 450以上の公共機関と3万以上の起業家が、“X－road”といわれているデータ交換レイヤーを利用
  - 80パーセントの自然人の収入申告が、電子的
  - 世界ではじめて電子投票を利用した国家

サイバー攻撃の時系列的記述

- 感情的対応
  - ４月２７日から２９日
- ４月27日の遅く
  - 政府のウェブサイトに対する最初の攻撃
- 「サイバー暴動」
  - ロシア語の掲示板などで、特定の引数をもちいたpingコマンドの利用が、指示/自動的にpingコマンドを発射する方法
- 主たる攻撃（４月３０日から５月１８日）
  - 大規模なボットネットの利用
  - 洗練-協調
    - インターネットのフォーラムによって指令や標的リストを伝えるという手法
  - ElionのDNSサーバとルーター
    - サービス障害
- 第１波（５月４日）
- 第２波（５月９日－１１日）
  - ５月９日（ロシアの戦勝記念日でもある）の攻撃は、熾烈
  - 58ものサイト-遮断
- 第３波（５月１５日）
- 第４波（５月１８日）

攻撃手法および攻撃目標
・攻撃元

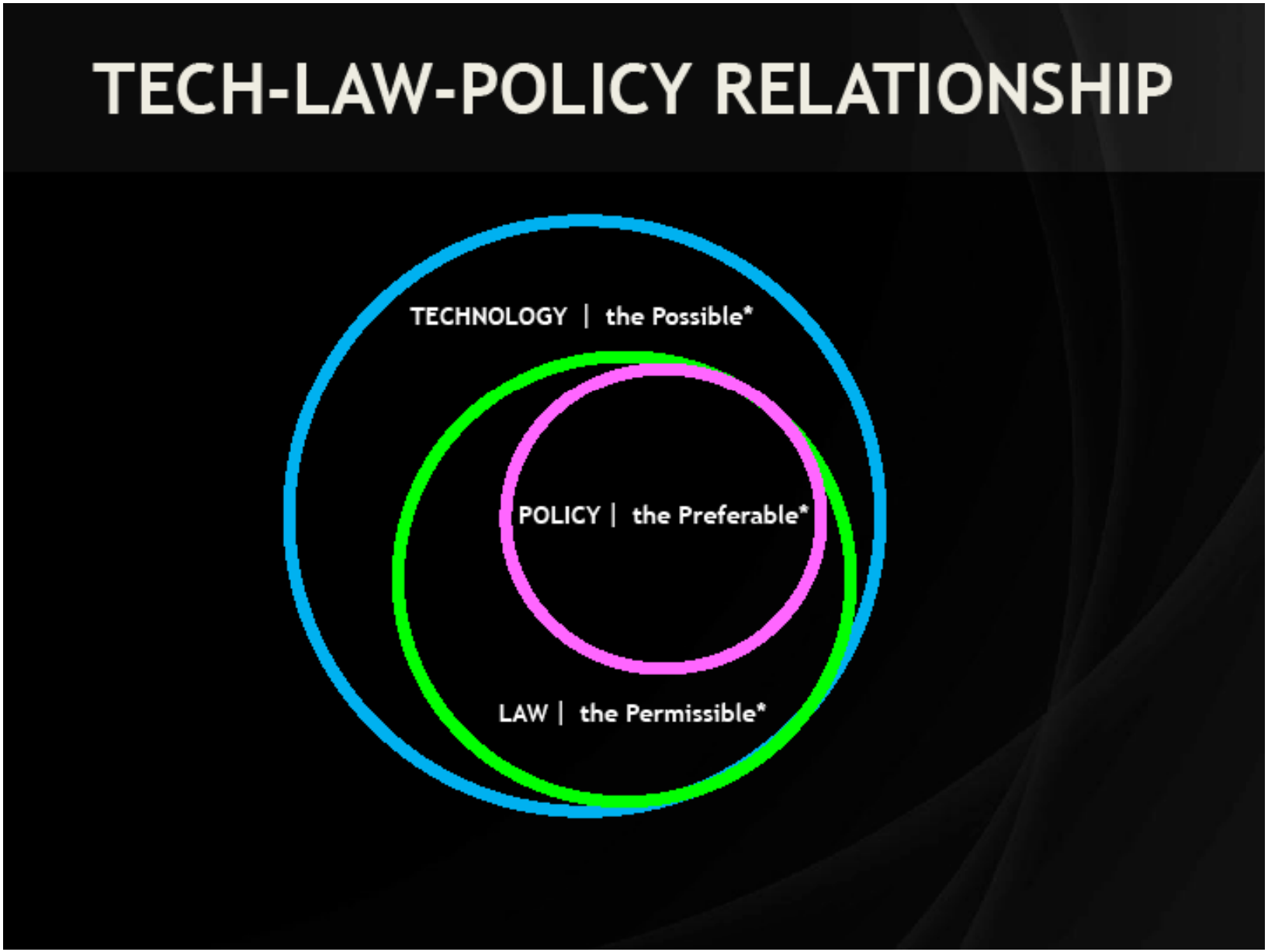
- 攻撃手法
  - DoSおよびDDoS攻撃
  - ウェブサイト改竄
  - DNSサーバ攻撃
  - 大量のスパム通信など
- 攻撃目標
  - エストニアのインターネット中枢-責任ある機構のサーバ
  - 政府および政治的ターゲット
  - 民間部門によって提供されるサービス
  - 個人的・ランダムな目標

- エストニアの外部から
- 煽動された大衆
  - フォーラム(http://2ch.ru)やウェブサイトの指示-国家主義的・政治的感情
- 主攻撃の第２波
  - 通常の市民の抗議行動の域を超えて
  - 中央の指令・コントロールが効いていた。
  - 波状攻撃は、定刻に行われ、金銭的・知的資源を有するもの

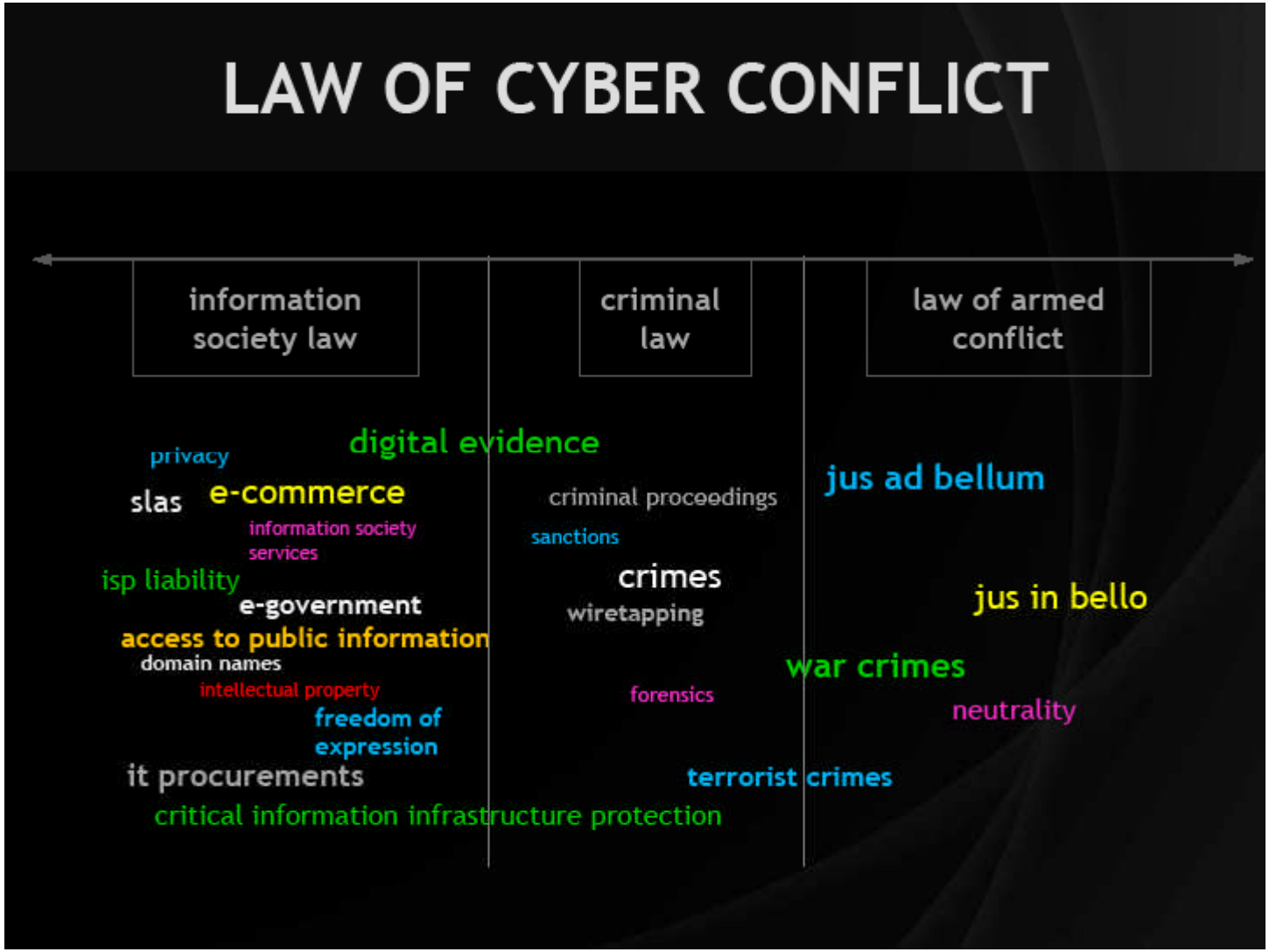
Day2 Sep.10 “Seminar”

- Session 3: Cyber Security Institutionalized – Pieces of an Effective Defence
  - Model International Organizations’ Legal and Policy Approaches to Cyber Incident
    - by Ms. Eneken Tikk, Estonia, CCD COE
      - IP addressは、パブリックデータなのか。日本の通信の秘密の悩みと一緒
  - 10.00 ICANN’s Developments in the Field of International Cyber Security
    - By Ms. Yurie Ito, Japan, Director of Global Security Programs for ICANN
  - 11.00 Public-Private Partnerships and National Input to International Cyber Security
    - By Ms. Maeve Dion, USA, GMU CIP
- 13.00 Session 4: Breakout

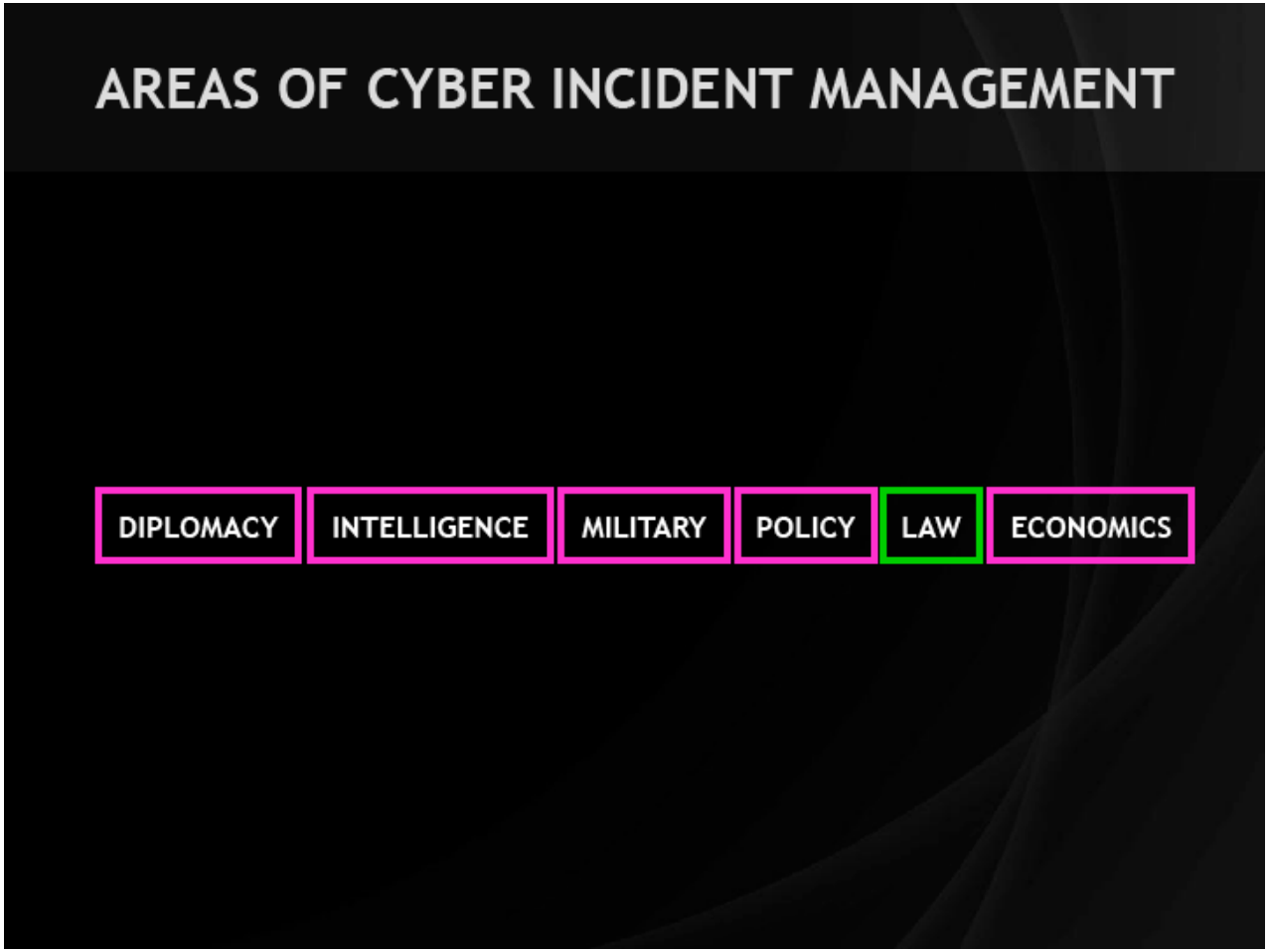
可能なこと、許容されること、望ましいこと



法のスペクトラム


LAW OF CYBER CONFLICT
information society law
criminal law
law of armed conflict
privacy
digital evidence
slas
e-commerce
criminal proceedings
jus ad bellum
information society services
sanctions
isp liability
crimes
e-government
wiretapping
jus in bello
access to public information
domain names
war crimes
intellectual property
forensics
neutrality
freedom of expression
it procurements
terrorist crimes
critical information infrastructure protection

対抗措置


AREAS OF CYBER INCIDENT MANAGEMENT
DIPLOMACY
INTELLIGENCE
MILITARY
POLICY
LAW
ECONOMICS

Day3 Sep.11.”Wrap up”

- 9.00 Enhanced Frameworks for International Cyber Security
  - Moderator: Prof. Thomas C. Wingfield, US Army Command and General Staff
- Law Enforcement Perspective
  - By Dr. Thomas Ramsauer, Germany, Federal Ministry of Interior National Defence Law
- Government’s Perspective
  - By Mr. Lauri Almann, Estonia, Aare Raig Attorneys-at-Law
- Information Society Law / User Perspective
  - By Prof. Lilian Edwards, UK, University of Sheffield

Day3 Sep.11.”Wrap up”-cont.

- 11.45 Observers’ Comments and Conclusions
  - Moderator: Prof. Julie Ryan, USA, George Washington University
  - Mr. Jason Healey, USA, Cyber Conflict Studies Association
  - Mr. John Bumgarner, USA, Research Director for Security Technology, U.S. Cyber Consequences Unit

感想

- 全般的にすばらしい参加者、講師、主催者
- 法律・ポリシの最先端の体験・議論を感じ取る。
- 「サイバー戦争」マネジメントの議論には最適であろう

- サイバー戦争概念がUS過ぎる気がする。ヨーロッパで開かれているのではあるが・・

Estonia 2010

- CCD CoE Conference on Cyber Conflict June 15-18, 2010
- すでにCFPがでています(11月末までです)
  - http://www.ccdcoe.org/conference2010/272.html
  - わが国のCCCプロジェクトや大量通信等ガイドラインについては、これを説明すべき時期にきているような気がする

Security Wars

- ネットワークのライトサイドとダークサイドの鬩ぎ合いをスターウォーズのアナロジーで解説する
- PacSecコンフェレンスでエピソード3やります
  - ダースベーダーになります。
- マイクロソフトのセキュリティページで大絶賛連載公表中