サイバー犯罪

グローバル化とサイバー化

インターネットの発達と犯罪

- 通常世界の犯罪は、サイバー空間でも犯罪
  ただし、技術上・政治上の異同により位相が異なる
- インターネットは、本質的に「国境」概念を持たない。→ネット上の「国境」の創出
- 統制側のネットワイドニング（統制拡張）が世界的な問題を引き起こす→監視
- マーケティング利用のSecurity化 →監視

「国境」の創出

- ゲートウェイ段階でのblocking（サーバで特定のIPアドレスへのアクセスを遮断）
- 自動filteringによる、特定傾向のcontentsの排除（→表現の自由と抵触）
- 自国内サーバに対する法執行機関による物理的／バーチャルな監視（トラッキングアプリケーションの導入義務、サイバーポリス、身分証明制度）

対抗措置の権利化（プライバシー）

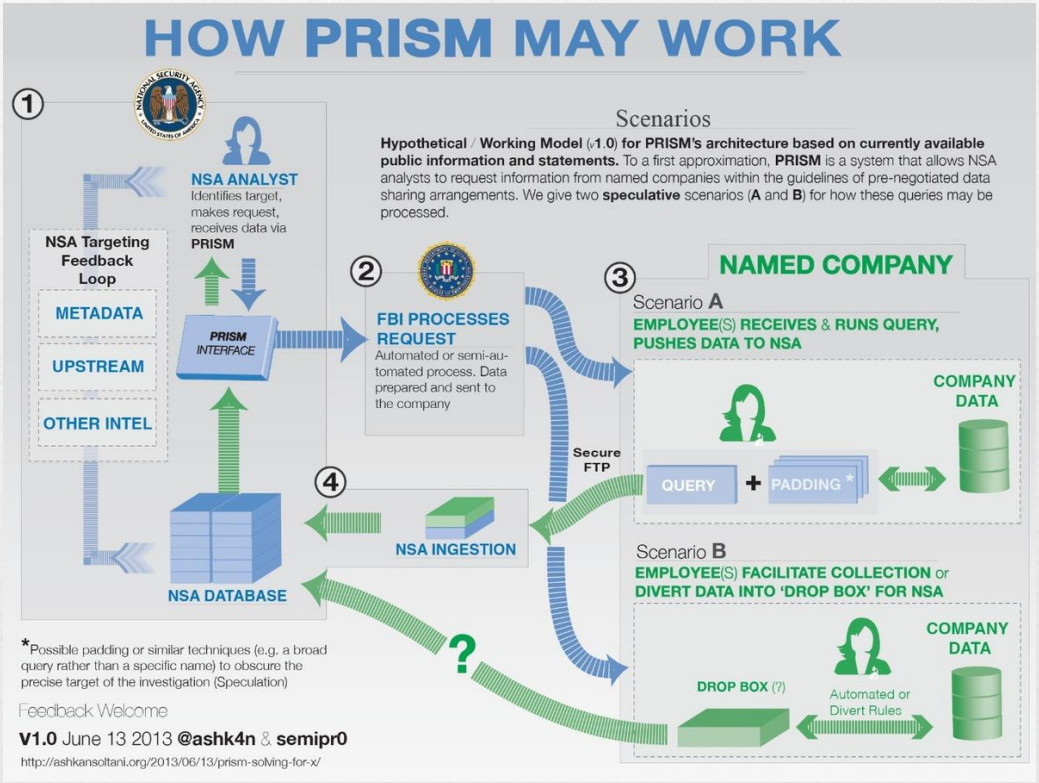
- 個人情報の自己コントロール権を基礎に、さらに発展
- プロキシサーバを利用した匿名化（TORなど）
- 暗号化による、本人認証、取引保護、信書（公開鍵＋暗号鍵方式の普及）（高bit暗号）
- プロバイダ業者等の秘匿義務→法執行機関による開示手続の簡易化
- 「忘れられる権利」：検索データからの削除

監視システムとサイバー空間

- 軍事監視体制：UKUSAによるECHELON（エシュロン）：軍事衛星（Intersat）を利用した、民間通信の傍受
→大時代的で時代遅れ、主に産業諜報に利用
- カーニボー：FBIにより導入された電子通信の総傍受システム
- PRISM：E.Snodenにより明らかにされたNSAによる通信総傍受システム

三沢基地の「像の檻」

PRISM


HOW PRISM MAY WORK
1
NSA ANALYST
Identifies target, makes request, receives data via PRISM
NSA Targeting Feedback Loop
METADATA
UPSTREAM
OTHER INTEL
PRISM INTERFACE
NSA DATABASE
Scenarios
Hypothetical / Working Model (v1.0) for PRISM's architecture based on currently available public information and statements. To a first approximation, PRISM is a system that allows NSA analysts to request information from named companies within the guidelines of pre-negotiated data sharing arrangements. We give two speculative scenarios (A and B) for how these queries may be processed.
2
FBI PROCESSES REQUEST
Automated or semi-automated process. Data prepared and sent to the company
3
NAMED COMPANY
Scenario A
EMPLOYEE(S) RECEIVES & RUNS QUERY, PUSHES DATA TO NSA
COMPANY DATA
QUERY
+
PADDING *
Secure FTP
4
NSA INGESTION
Scenario B
EMPLOYEE(S) FACILITATE COLLECTION or DIVERT DATA INTO 'DROP BOX' FOR NSA
COMPANY DATA
DROP BOX (?)
Automated or Divert Rules
?
*Possible padding or similar techniques (e.g. a broad query rather than a specific name) to obscure the precise target of the investigation (Speculation)
Feedback Welcome
V1.0 June 13 2013 @ashk4n & semipr0
http://ashkansoltani.org/2013/06/13/prism-solving-for-x/

サイバー空間での被害

- 自己情報の流出→行政機関・企業経由の流出（広範さ、影響や被害算定の困難さ）
- SNS等での誹謗・中傷→情報開示問題
- サイバー空間でのヘイトスピーチ問題（国際性を持つ）
- 著作権問題（ただし、これは著作権がデジタル、サイバー空間などを想定していない古い制度であるため）→YouTube等、リッピング、キャッシュ、TV配信等
- マルウェア被害（世界的）cf. パキスタン

マルウェア

- ウィルス：感染し、自己増殖。データやアプリケーションを破壊
- ワーム：自己増殖。リソース等を枯渇させる
- トロイの木馬：実行されると、コンピュータ上の秘匿情報を外部に送信する
- その他：自己の削除を抑制させ、機器の警告表示等を支配下に置くマルウェアなど

情報詐取のシステム的側面

- 本来、テキストだけでは、感染は発生しない。
- ウェブ上のスクリプト等は、アプリケーションとして作動するため、JAVAスクリプト、WindowsのWHSやVBScript Jscriptなどに感染プログラムをしのばせることが可能
- WWW／http、ftp、smtpなどTCP/IP上のプロトコルは、対話（dialogue）によって機器同士が通信する→偽装対話による情報詐取

ネットワーク攻撃

- DoS攻撃等：同一サーバに繰り返しリクエストを送信し続ける
- ポートスキャニング：ネット接続部分の穴を総当たりで検出→脆弱性（vulnerability）
- 詐欺サイト：Webスクリプトによりアクセスした機器の情報を詐取
- DNSキャッシュポイズニング：DNS偽装により、詐欺サイトに誘導

サイバー空間の法は未成熟

- 自己防衛のための手段が侵害技術化
- 本来的にグローバルなので、国内規制を基本とする組織犯罪対策なども無意味になっていく
- 旧体制の利権保護が、サイバー技術を制限しようとする強い傾向（DRMなど）
- 監視対象は拡大するが、監視主体は存在しない。システム的監視（「第三世代監視」）
- 情報技術のブラックボックス化により、過度に脆弱な層が生じる
  →新たな段階のデジタルデバイド