Q&A 5月7日 分

インターネット工学概論

1. 選挙の時に、アルゴリズムを利用して、情報をコントロールしていた疑惑があることに驚いた。一般の人はこの事実に気付きようがないと感じたが、実際どのように利用者側として、情報が故意にコントロールされていることに気づけば良いのか気になった。
   ➔情報のソース(生成者)の証明を、流通するコンテンツに付与するという 研究開発・政策が進められています。 **TrustedWeb＠内閣府、C2PA Content Credentials standard by CAI(Contents Authenticity Initiative)** などが あります。
   ➔他の関連する情報の洪水を発生させて、重要な本当の情報を見えにくくする 方法も常套手段として 使われていますね。

2. 授業中に、セキュリティとブロックチェーンの関連に話があったが、過半数の人が信用できる人がいるとブロックチェーンが壊れるということとセキュリティーがどう関連しているのかがわからなかったので、もう一度説明していただけないでしょうか。
   ➔多数決なので、半分以上が仲間になると操作が可能になってしまいます。絶対多数(過半数)を持たない個人やグループの集合体での意思決定という仕組みがブロックチェーンです。過半数を乗っ取られると、破綻します。
   ➔「科学は嘘をつかない」、「科学には多数決が存在しない」。。。。。

3. Storage centricといういお話がありました。データの輸送コストの点やセキュリティの点からこれが有効であることは理解しましたが、コンピュータをデータの近くに持っていくということはデータセンタの近くでしかコンピュータを操作できないということでしょうか
   ➔ コンピュータをデータが存在する場所に 移動させる・生成する ですね。

4. アクティブサイバーディフェンスは事前に対応策を作っておくことだと認識してしましたが、なぜ日本では前もって相手に攻撃するという認識が広まってしまっているのでしょうか。
   ➔ 不思議ですねぇ。。。。。。。。

5. セキュリティにおける本当の攻撃者は保守的人種だという考えにハッとさせられました。僕も特に歳を取った時老害的な挙動はしないように気をつけようと思いました。
   ➔ はい。気を付けましょう。。。でも、当事者になると忘れちゃうんですよねぇ。

6. 安心と安全の違いについての話がわかりやすく興味深かったです。セキュリティへの誤った考え方として風紀委員の強化が挙げられていましたが、これは法律を整備することとは異なるのでしょうか？
   ➔法律は一番強い(変更に時間も要する)方法です。条例がその次。あとは、ソフトロー(Soft Law)と呼ばれる 弱い(柔らかい)規制です。 監視の頻度・粒度・強制度が異なりますね。
   ➔風紀委員は、個人としての裁量性があって、運用の形態が変わります。これは、明るい面と暗い面の両方がありますね。裁量が強すぎるのは、暗い面が出やすいかな。。。

7. 「完全0を目指すと碌なことがない」というのはまさにその通りだと思いました。

8. どんな対策にも長所と短所があるということはしっかり頭に入れます。
   ➔ Dark-side と Brighter-sideがいつもありますので。

8. 無理に禁止するとブラックマーケットが生まれるという考え方はめっちゃ共感できます。
9. 単純なactiveな行動がさらなる問題を引き起こす可能性があるので、proactiveな行動、つまり事前に問題を予測して対応を講じるとともに、予想外の問題が生じた時も柔軟に対応することが大切だと知った。事前に対応することについてはプロが行うことができるが、予想外の問題に柔軟に対応することはユーザー側に求められることなので、ある程度の知識が必要であるということですか？

   ➔ ユーザがある程度のリテラシーを持っているのが 理想的ですね。いざときの対応能力を持った人材が、もっとも 重要な人材になりますね。
10. 事故は一定数起こらないと必要性が認知されないため経済的に儲からなくなるがそれでも事故を起こすべきでないものは法律で決めていくと言う話が印象に残った。例えばインフラは事故が起こらないうちはありがたみが分からずそう言うことに財政を使ってる人のありがたみがわからないと言うことも起こると思うので難しいなと感じた。

    ➔はい。この説得をできるかが、とてもとても 難しいですね。

    ➔研究も実は、よく似ています。顕著な結果が出なければ、潰したくなるのが 多くの経営者。 利益を出さない ＝ インシデント(＝計算されていない支出)が発生しない。

    ➔結局は、短期利益を重視するか？　中長期利益を重視するか？

11. 為政者が善悪に厳格すぎると、かえって不都合が生じるという話を聞いて、違法サイト「漫画村」を思い出しました。違法に漫画を読むのは悪ですが、漫画家にとって一人でも多くの人に作品を読んでもらうことが何よりのやりがいでもあります。
    ➔ その話は、お聞きしています。
12. 完全な安全を求め規制をすると、陰で違法な取引が生まれ状況が見通せなくなり却って危険だという話は、矛盾を孕んでて面白かった。一方で、オープンソースとブラックボックスの話で、ブラックボックスにしないとセキュリティが実現されないという話もあった。違法なことをしてる人が検挙されないために身を隠してることもあるし、安全のために仕組みが隠されていることもある。第三者から見るとどちらもただのブラックボックスなので、悪意のものなのか善意のものなのか、判断がつかなくなると怖いと思った。
13. 厳密すぎないセキュリティの方がかえって安全なのだという視点が驚きだった。これはインターネットに限らず古今東西ありとあらゆる規制について言えることだなとおもった。
14. サイバーセキュリティにおいて保守的なかんがえがダメというのはその通りだと思いました。完全に締め付けるのはだめで、ある程度の余白を持たせること、そして、適度な事故が必要であること、、など納得が多かったです。自分が子育てするときもそのようにしようと思いました。

15. セキュリティ対策を行うことによって安全が担保される代わりに個人の利益や安全、自由が損なわれてしまうことについてとても考えさせられた。

例えば、防犯カメラを設置することは犯罪の抑止になる一方で、常時監視されることで個人の行動や選択の自由が制限されてプライバシーが損なわれてしまったり、政府によるインターネットの検閲やフィルタリングは過激思想を抑え込み、政府の体制を崩されることを防ぐことができるかもしれないが、市民の情報のアクセスや報道、言論の自由が奪われてしまったりすることがある。

これらは全て不特定多数の人の自由を制限するものであるため、セキュリティ対策をする際は社会的な合意が必要なのだと思った。

➔ツールは、使い方で、悪い作用をする場合と、良い作用をする場合がありますね。

「悪い作用」があるので、そのツールを使用禁止にするのは？

「悪い作用」は、そのツールを作った人の責任にすべき？