

An aerial photograph of a city, likely New York City, with a blue color overlay. A large, semi-transparent blue letter 'G' is positioned on the right side of the image. The text is white and centered in the lower half of the image.

Never Gonna Give you up, Never Gonna Let You Down: From Hacking to Cyberwar

Marc Rogers, VP Cybersecurity Strategy, Okta

Never Gonna Give you up.

./whoami

**Marc Rogers,
AKA Cyberjunky AKA Cjunky AKA CJ**

- I am a Hacker
- I am the VP of Cybersecurity Strategy at Okta
- I am a security researcher (Tesla, TouchID, Glass etc)
- I designed hacks for USA's Mr Robot
- I am the Head of Security for DEF CON
- I have too many hats

./whoami

Mostly, I just like to break stuff.

Never Gonna Let You down.

How did we get from here.....



To here?



So, how **did** we?

1. Everything became connected?
2. Global and social media allowing mass reach?
3. We were too successful finding bugs and making tools?

Maybe we have been here all along, and all that has changed is **Volume, Variety and Velocity**.

Cyber/Information warfare has changed the battlefield.

- Nations have an unprecedented reach for minimal investment.
- Attacks can be launched with greatly reduced risk.
- Ammunition is cheap and targets are readily available
- **Waging asymmetric warfare has never been easier.**

Never Gonna Run around and Desert You.


We understand Cyber warfare and it's accelerating.

WIRED




ANDY GREENBERG 06.28.19 6:09 PM SECURITY

Iranian Hackers Launch a New US-Targeted Campaign as Tensions Mount

Three cybersecurity firms have identified phishing attacks stemming from Iran—that may lay the groundwork for something more destructive.



Iran's Revolutionary Guard Corps.



  


POLICY / CIVILIZATION & DISCONTENTS

US hack attack hobbles Iran's ability to target oil tankers, NYT says


Despite the results, some Trump officials question if costs outweigh benefits.

by Dan Goodin - Aug 29, 2019 4:20am CST

 Login to bookmark  46




Commercial oil tanker AbQaiq in 2003.

 US Navy

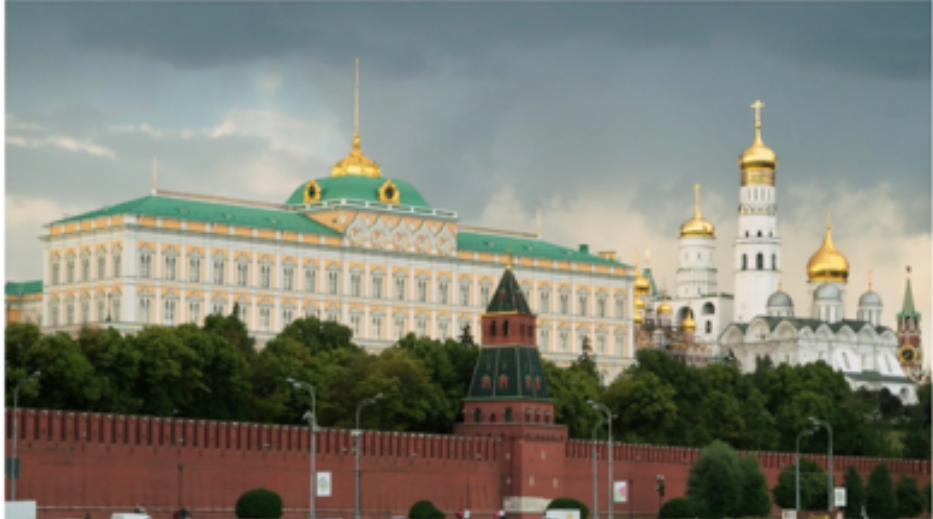
Hackers working for the US government wiped out a database and computer systems that Iran's paramilitary arm used to plan attacks against oil tankers in the Persian Gulf, [The New York Times](#) reported on Wednesday.

The attack occurred on June 20, the same day that [President Trump](#) called off a retaliatory airstrike after Iran shot down a US drone. Iran is still trying to recover information destroyed in the attack and to restart Iranian computer systems and military communications networks that were taken offline, Wednesday's report said.

MIT Technology Review 

Computing Aug 5

Russian hackers are infiltrating companies via the office printer

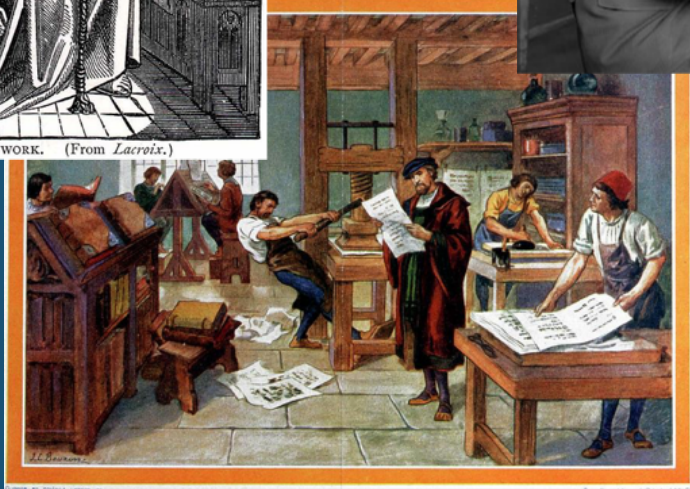


A group of hackers linked to Russian spy agencies are using "internet of things" devices like internet-connected phones and printers to break into corporate networks, Microsoft announced on Monday.

But, we need to better understand Information Warfare

- **We are already in the age of Information Warfare**
- Rather than encryption ending the GOLDEN age of SIGINT it pushed collection to the endpoints and started the PLATINUM age.
- Data drives influence, influence is a weapon.
- Well designed information warfare campaigns are self propagating highly affect truly asymmetric methods of attack.

Information: We have come a long way in a short time.



The power of Influence



Twitter profile of Theresa May (@theresa_may). The profile picture shows her smiling. A gear icon is in the top left, and a 'Follow' button is in the top right. Below the name and handle is a bio: 'Prime Minister and @Conservatives Leader.' A status 'DOES NOT FOLLOW YOU' is displayed. At the bottom, statistics show 1,365 Tweets and 752,747 Followers.

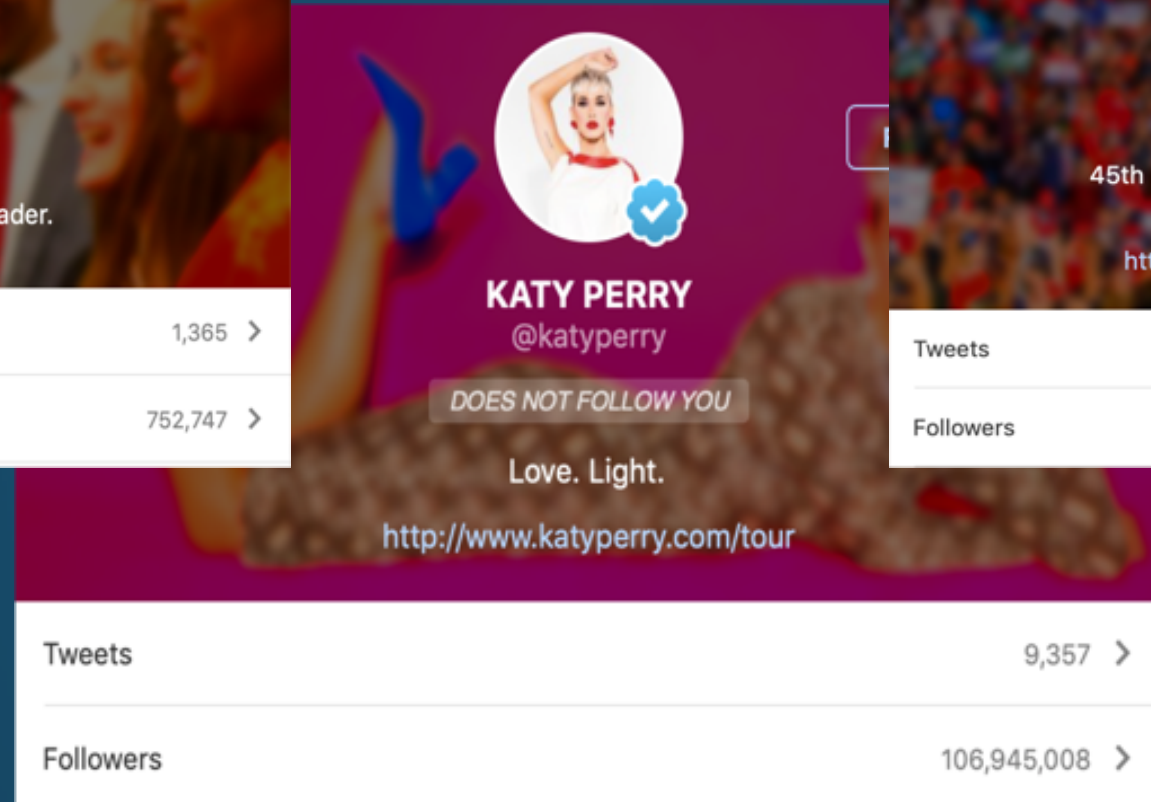
Theresa May
@theresa_may

Prime Minister and @Conservatives Leader.

DOES NOT FOLLOW YOU

Tweets 1,365 >

Followers 752,747 >



Twitter profile of Katy Perry (@katyperry). The profile picture shows her in a white dress. A gear icon is in the top left, and a 'Follow' button is in the top right. Below the name and handle is a bio: 'Love. Light.' and a link 'http://www.katyperry.com/tour'. A status 'DOES NOT FOLLOW YOU' is displayed. At the bottom, statistics show 9,357 Tweets and 106,945,008 Followers.

KATY PERRY
@katyperry

Love. Light.

<http://www.katyperry.com/tour>

DOES NOT FOLLOW YOU

Tweets 9,357 >

Followers 106,945,008 >



Twitter profile of Donald J. Trump (@realDonaldTrump). The profile picture shows him. A gear icon is in the top left, and a 'Follow' button is in the top right. Below the name and handle is a bio: '45th President of the United States of America' and 'Washington, DC'. A link 'http://www.Instagram.com/realDonaldTrump' is provided. A status 'DOES NOT FOLLOW YOU' is displayed. At the bottom, statistics show 40,400 Tweets and 57,755,775 Followers.

Donald J. Trump
@realDonaldTrump

45th President of the United States of America 🇺🇸
Washington, DC

<http://www.Instagram.com/realDonaldTrump>

DOES NOT FOLLOW YOU

Tweets 40,400 >

Followers 57,755,775 >

70% of millennials said they feel more excited about doing things when their friends agree with it and 68% said they usually do not make major decisions without discussing it with people they trust.

The background is a solid dark blue color. It features several faint, light blue circular patterns and arrows. In the top right, there is a large circular pattern with concentric circles and a dashed outer ring with an arrow pointing clockwise. In the bottom right, there is a smaller circular pattern with concentric circles and a dashed outer ring with an arrow pointing clockwise. In the bottom left, there is a circular pattern with concentric circles and a dashed outer ring with an arrow pointing clockwise. In the top left, there is a small circular pattern with concentric circles and a dashed outer ring with an arrow pointing clockwise.

Never Gonna Make You Cry.

Common information warfare strategies



Distort



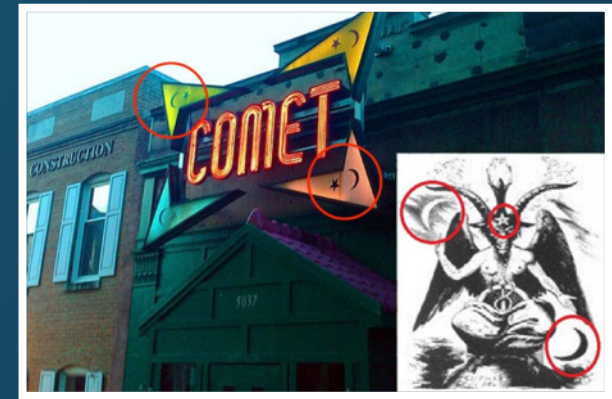
Dismiss



Distract



Divide



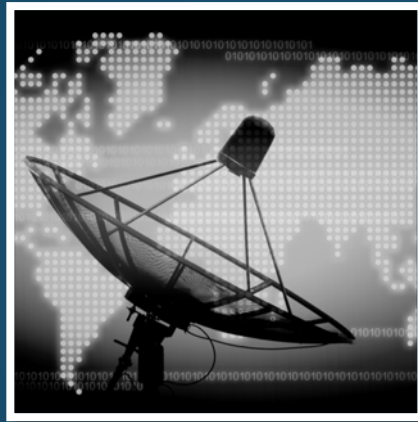
Dismay

NATIONAL INSTRUMENTS OF INFLUENCE

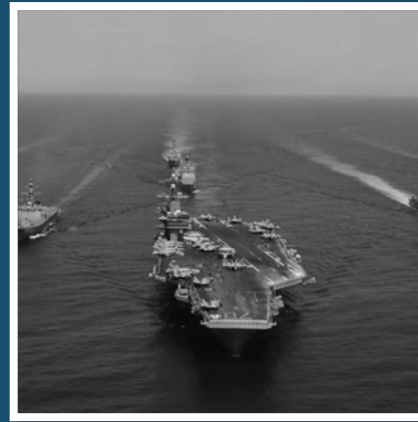
Resources available in pursuit of national objectives...



Diplomatic



Informational



Military



Economic

...and how to influence other nation-states.

BUSINESS INSTRUMENTS OF INFLUENCE

Resources available in pursuit of corporate objectives...



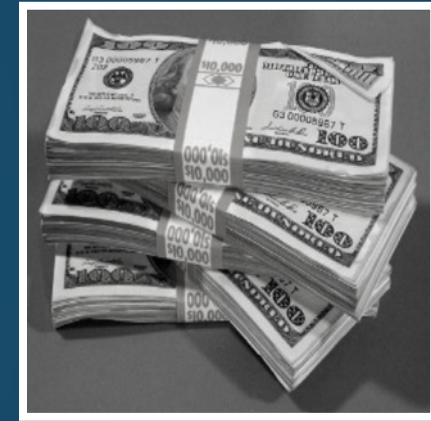
**Business Deals &
Strategic
Partnerships**



**PR and
Advertising**



**Mergers and
Acquisitions**



**R&D and Capital
Investments**

Prejudice, Misinformation and Fear can turn a simple Information display bug into a critical vuln

Would you ride in a car or fly in a plane with this on the infotainment unit?



**THE
COUNTDOWN
HAS BEGUN**

الله أكبر

00 : 00 : 05

Never Gonna Say Goodbye.

Hackers are legitimate targets now?

- As “Enemy Combatants” kinetic options are firmly on the table..

In a Cyber War Is It OK to Kill Enemy Hackers?

Welcome to the brave new world of cyber warfare.

DOMINIC BASULTO 11 April, 2013



The new **Tallinn Manual on the International Law Applicable to Cyber Warfare**, which lays out 95 core rules on how to conduct a cyber war, may end up being one of the most dangerous books ever written. Reading through the Tallinn Manual, it's possible to come to the conclusion that - under certain circumstances - **nations have the right to use "kinetic force" (real-world weapons like bombs or armed drones) to strike back against enemy hackers.** Of course, this doesn't mean that **a bunch of hackers in Shanghai** are going to be taken out by a Predator Drone strike anytime soon - but it does mean that a nation abiding by international law conventions - such as the United States - would now have the legal cover to deal with enemy hackers in a considerably more muscular way that goes well beyond just **jawboning a foreign government.**

Welcome to the brave new world of cyber warfare.

Location: Syria



TALLINN MANUAL ON THE INTERNATIONAL LAW APPLICABLE TO CYBER WARFARE

The product of a three-year project by twenty renowned international law scholars and practitioners, the *Tallinn Manual* identifies the international law applicable to cyber warfare and sets out ninety-five 'black-letter rules' governing such conflicts. It addresses topics including sovereignty, State responsibility, the *jus ad bellum*, international humanitarian law, and the law of neutrality. An extensive commentary accompanies each rule, which sets forth each rule's basis in treaty and customary law, explains how the Group of Experts interpreted applicable norms in the cyber context, and outlines any disagreements within the group as to each rule's application.

The Director of the Project, Professor **MICHAEL N. SCHMITT**, is Chairman of the International Law Department at the United States Naval War College.

THE VERGE

TECH SCIENCE ENTERTAINMENT MORE



POLICY

Killing hackers is justified in cyber warfare, says NATO-commissioned report

128

By Aaron Souppouris | Mar 21, 2013, 6:09am EDT

Via Engadget and TechWeek Europe | Source The Guardian, NATO Cooperative Cyber Defence Centre of Excellence, and Tallinn Manual on the International Law Applicable to Cyber Warfare | Image Instacod.es

f t SHARE

```
int bitsLeft = 0;
int count = 0;
for (const uint8_t *ptr = encoded; count < bufSize && ptr; ++ptr) {
    uint8_t ch = *ptr;
    if (ch == '\t' || ch == '\r' || ch == '\n' || ch == '\0') {
        continue;
    }
    buffer <<= 5;
    // Deal with commonly mistyped characters
    if (ch == '0') {
        ch = 'O';
    } else if (ch == '1') {
        ch = 'L';
    } else if (ch == '8') {
        ch = 'B';
    }
    // Look up one base32 digit
    if ((ch >= 'A' && ch <= 'Z') || (ch >= 'a' && ch <= 'z')) {
        ch = (ch & 0x1F) - 1;
    } else if (ch >= '2' && ch <= '7') {
        ch -= '2' - 26;
    } else {

```

Hackers have always been targets

CCC/DOB 1989. Karl Koch, Marcus Hess, Hans Hübner

SPIEGEL ONLINE SPIEGEL

Menü | Politik Meinung Wirtschaft Panorama Sport Kultur Netzwelt Wissenschaft mehr ▼

EINESTAGES Schlagzeilen | DAX 11.701,02 | Abo


Nachrichten > einestages > Hacker > Karl Koch alias Hagbard Celine: Tod eines Hackers

Daten, Drogen, Verschwörungstheorien

Einer der ersten deutschen Hacker - der mysteriöse Tod des Karl Koch

In einem Wald bei Celle verbrannte Karl Koch, mit 23 Jahren am 23. Mai 1989. Er wählte sich auf der Spur der Illuminaten und verkaufte dem KGB Daten der US-Regierung. Tragödie oder Kriminalfall?

Von Frank Patalong ▼



Fotos

Geschichte | Der KGB-Hack c't Retro 2018 S. 60




Bild: Thorsten Hübner

Der KGB-Hack

Wie Ende der 80er-Jahre fünf deutsche Hacker in die Mühlen der Geheimdienste gerieten

Pengo, Pedro, Urmel, DOB und Hagbard Celine – diese Pseudonyme stehen für die wohl kurioseste Hacker-Geschichte kurz vor dem Ende der alten BRD. Die Gruppe um Karl Koch drang in internationale Rechnernetze ein und verkaufte raubkopierte Software an den russischen Geheimdienst. Zum Verhängnis wurde ihr eine riesige Datei, die angeblich Details zur SDI-Raketenabwehr der USA enthalten sollte.

Von Detlef Borchers

Never Gonna Tell a Lie and Hurt You.

Defense: We need to rethink our understanding of impact.

- We now need to think about vulnerabilities from three angles.
- Cyber
- Physical
- Cognitive

Defense: We need to rethink classification of Vulns.

Scoring methods to classify vulnerabilities are inadequate

- We allocate resource and priority based on an incomplete picture

However in the last 10 years the game has changed

- Much of our impact assessment comes from control of a system
- However the picture is much bigger now
- “LOW” bugs can no longer be assumed to be LOW
- “Informational” bugs might actually be HIGH
- Displaying the wrong message could be CRITICAL

We really need context and intelligence to accurately classify bugs.

Defense: Agents of Change

Hackers working to change the landscape.

Katie Moussouris

Sara-Jayne Terp

Katie Moussouris

Wassenaar – In 2013 41 countries revised the Wassenaar agreement to regulate export of “Intrusion Software” and “Intrusion software technology”

Katie & Iain Mulholland representing the US State Department worked to renegotiate the scope.

Its thanks to their work that we don't have to fill out export license applications for vulnerability disclosure or incident response.

Sara-Jayne Terp

Credibility Coalition – Disinformation Working Group

The Credibility Coalition's Misinfosec Working Group ("MisinfosecWG") maps information security (infosec) principles onto misinformation. Current work is to develop a tactics, techniques and procedures (TTP) based framework that gives misinformation researchers and responders a common language to discuss and disrupt misinformation incidents.

Thanks also to **Pablo Breuer** of SOCOM/Donovan Group for his efforts supporting this work and being a general inspiration!

Planning

Strategic Planning

4Cs

Facilitate Story Propaganda

Leverage Existing Narratives

Competing Narratives

Objective Planning

Center of Gravity Analysis

Create Master Narratives

Preparation

Develop People

Create fake Social Media Profiles / Pages / Groups

Create fake or impersonation sites

Create fake experts

Develop Networks

Cultivate useful idiots

Hijack legitimate accounts

Use concealment

Create fake web sites

Create funding campaigns

Create #hashtag

Microtargeting

Clickbait

Promote online funding

Paid targeted ads (e.g. Facebook)

Develop Content

Generate information pollution

Troll content

Memes

Conspiracy narratives

Exposé facts

Create fake videos and images

Leak filtered documents

Create fake research

Adapt Existing Narratives

Create Competing Narratives

Channel Selection

Manipulate online polls

"Backstage" personas

YouTube

Reddit

Instagram

LinkedIn

Pinterest

WhatsApp

Facebook

Twitter

Execution

Pump-Priming

Sift Legitimate Influencers

Demand Unimpeachable Proof

Deny Involvement

Surrender of Truth

Use SMS/WhatsApp/Chat Apps

Seed Distortions

Use Fake Experts

Search Engine Optimization

Exposure

Mimic Social Media as a Political Force

Cover Online Opinion Leaders

Flooding

Oversteering Domestic Social Media Ops

Fabricate Social media Comment

Tertiary Sites Amplify News

Twitter 'Troll' Amplify and Manipulate

Twitter Bot Amplify

Use #hashtag

Dedicated Channels disseminate information pollution

Go Physical

Organize Remote rallies and events

Persistence

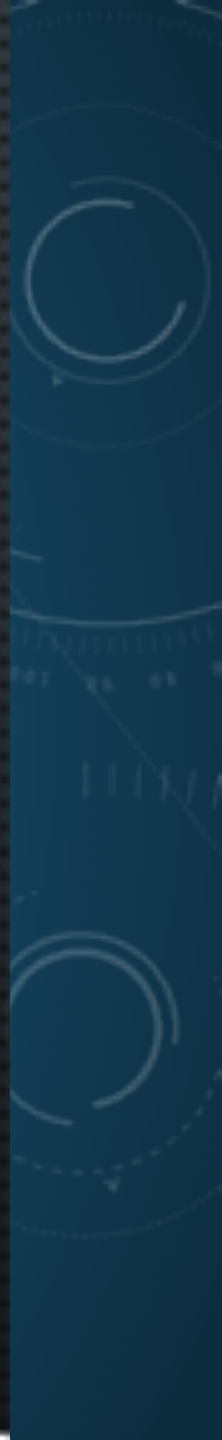
Legacy Web Content

Play the Long Game

Continue to Amplify

Evaluation

Measure Effectiveness



Never Gonna Tell a Lie and Hurt You.

Conclusion

Hacking – Has always been part of warfare, its just had different names at different periods of time.

Hackers – Will always be the best equipped at offense and defense because it is part of who we are.

Hackers - We have to help the landscape change in responsible, less risky ways. This means building trust.

Hackers – We need to recognize that actions have greater impact than ever before. You can literally get killed for the wrong decision.

An aerial photograph of a city, likely Dubai, featuring a complex highway interchange and several tall skyscrapers. The entire image is overlaid with a semi-transparent blue filter. The text "Thank You" is centered in the middle of the image in a white, sans-serif font.

Thank You

Goodbye.

