

HACKING & TROLLING **THE CHANGING FACE** **OF HACKTIVISM IN** **THE DISINFORMATION** **AGE**

iDefense Threat Intelligence

Mei Nelson

December 11, 2019



LEGAL NOTICE & DISCLAIMER

© 2019 Accenture.

ACCENTURE SECURITY

Accenture Security helps organizations build resilience from the inside out, so they can confidently focus on innovation and growth. Leveraging its global network of cybersecurity labs, deep industry understanding across client value chains and services that span the security lifecycle, Accenture protects organizations' valuable assets, end-to-end. With services that include strategy and risk management, cyber defense, digital identity, application security and managed security, Accenture enables businesses around the world to defend against known sophisticated threats, and the unknown. Follow us [@AccentureSecure](https://twitter.com/AccentureSecure) on Twitter or visit us at www.accenture.com/security.

This document is produced by consultants at Accenture as general guidance. It is not intended to provide specific advice on your circumstances. If you require advice or further details on any matters referred to, please contact your Accenture representative.

The opinions, statements, and assessments in this report are solely those of the individual author(s) and do not constitute legal advice, nor do they necessarily reflect the views of Accenture, its subsidiaries, or affiliates.

WHO AM I

Mei Nelson

Security Principal

Geopolitical and Strategic
Intelligence Team

iDefense Threat Intelligence

Accenture Security

Accenture



HACKER – HACKTIVIST – HACKTIVISM

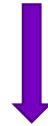
Hacker



Hacktivist

Hacker + Activist

Combines traditional activist tactics with hacking techniques



Hacktivism

Using hacking skills to spread a specific message and bring attention to a political or social cause

or

The use of malicious cyber activities by non-state actors for ideological purposes (iDefense)

HACKTIVISM

Decline?

hacktivism decline

About 225,000 results (0.43 seconds)

The phenomenon of internationally-coordinated and politically-motivated cyber attacks has dramatically **declined** in the last three years, according to a new study. Analysts at Recorded Future found that the number of active **hacktivist** groups has more than halved since 2016, falling from 27 to just eight last year. Aug 21, 2019

Why is the number of active hacktivist groups plummeting ...
<https://tech.newstatesman.com/security/hacktivist-groups>

hacktivist

The Decline of Hacktivism: Attacks Drop 95 Percent Since 2015
<https://securityintelligence.com/posts/the-decline-of-hacktivism-attacks-...>
May 16, 2019 - Yet amid all the concern, there is one threat trend that our data suggests has been on the **decline**: **hacktivism** — the subversive use of ...

Return to Normalcy: False Flags and the Decline of ...
<https://www.recordedfuture.com/international-hacktivism-analysis>
Aug 21, 2019 - In addition, **hacktivism** has taken a back seat in news reporting, and general mentions seem to be in **decline**. Insikt Group® utilized the ...

Hacktivism in decline as it returns to its roots | BetaNews
<https://betanews.com/2019/08/21/hacktivism-in-decline>
Aug 21, 2019 - **Hacktivism** has its origins in small groups of people banding together to achieve common goals. In recent years, however, it's become ...

Sorry script kiddies, hacktivism isn't cool anymore: No one ...
https://www.theregister.co.uk/hacktivism_in_decline_recorded_future
Aug 21, 2019 - The youthful doings of US presidential wannabe Beto O'Rourke are in sharp **decline**, according to threat intel biz Recorded Future, which ...

Hacktivist attacks dropped by 95% since 2015 | ZDNet
<https://www.zdnet.com/article/hacktivist-attacks-dropped-by-95-since-2015>
May 17, 2019 - According to IBM, security incidents caused by hacker groups operating under **hacktivism** causes has been on a **decline** since 2015, when the ...

Source: Google



Source: cDC

The Cult of the Dead Cow - the Dead Cow Died?

HACKTIVISM

Changing Face?



Source: Wikimedia

THE CHANGING FACE OF **Hacktivism**

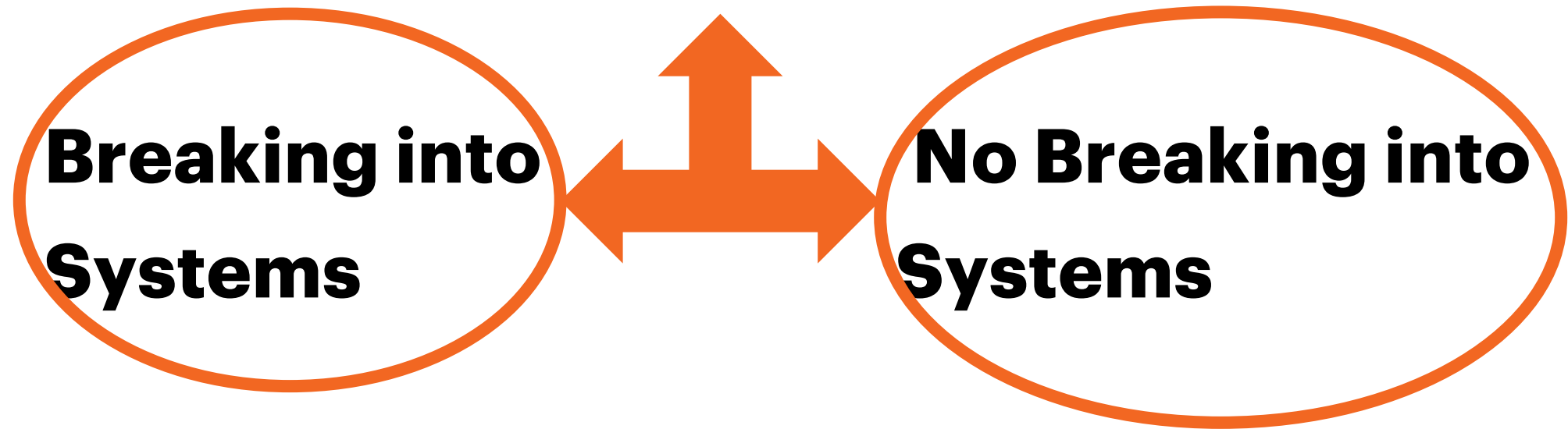
Non-state Actors



State Actors

THE CHANGING FACE OF **Hacktivism**

Malicious Cyber Activities





HACKTIVISM **&** **THE DISINFORMATION AGE**

INFORMATION OPERATIONS

THREE TYPES & THREE DIMENSIONS



DISINFORMATION OPERATIONS

GOALS: THE “D” WORDS

DIVIDE

DISCREDIT

DISTRACT

DENY

DISINFORMATION OPERATIONS METHODS

“WHITE” METHOD

Broadcasting one’s message openly through state media

“GRAY” METHOD

Placing information in other sympathetic media

“BLACK” METHOD

Using hackers, trolls, and honeypots

DISINFORMATION OPERATIONS TACTICS

- Flooding the media with multiple versions of a story to confuse the audience
- Publicizing scandalous information to discredit a critic or adversary
- Distracting world opinion from negative information, by highlighting or even creating some other crisis or scandal
- Using inauthentic social media profiles to inflame real-world violence by publicizing rallies of rival groups

CYBER-ENABLED INFORMATION OPERATIONS

Broadly

Any information operations taking place in cyberspace, including in online media and social media

Narrowly

Information operations leveraging offensive cyber threat activity such as subverting secure system

CYBER-ENABLED INFORMATION OPERATIONS

Hacktivism

**Non-state actors for
ideological purposes**

**State-controlled
hacktivism using false
personas**

**State-encouraged
hacktivism trolling**

CASE STUDY: #MACRONLEAKS (PART I)

- Disinformation campaign: rumors, fake news, forged documents
- Offensive network intrusion: computers of Macron's campaign staff
- Spreading stolen data using trolls and bots



Source: Reuters

CASE STUDY: #MACRONLEAKS (PART II)

SNAKEMACKEREL (APT 28)

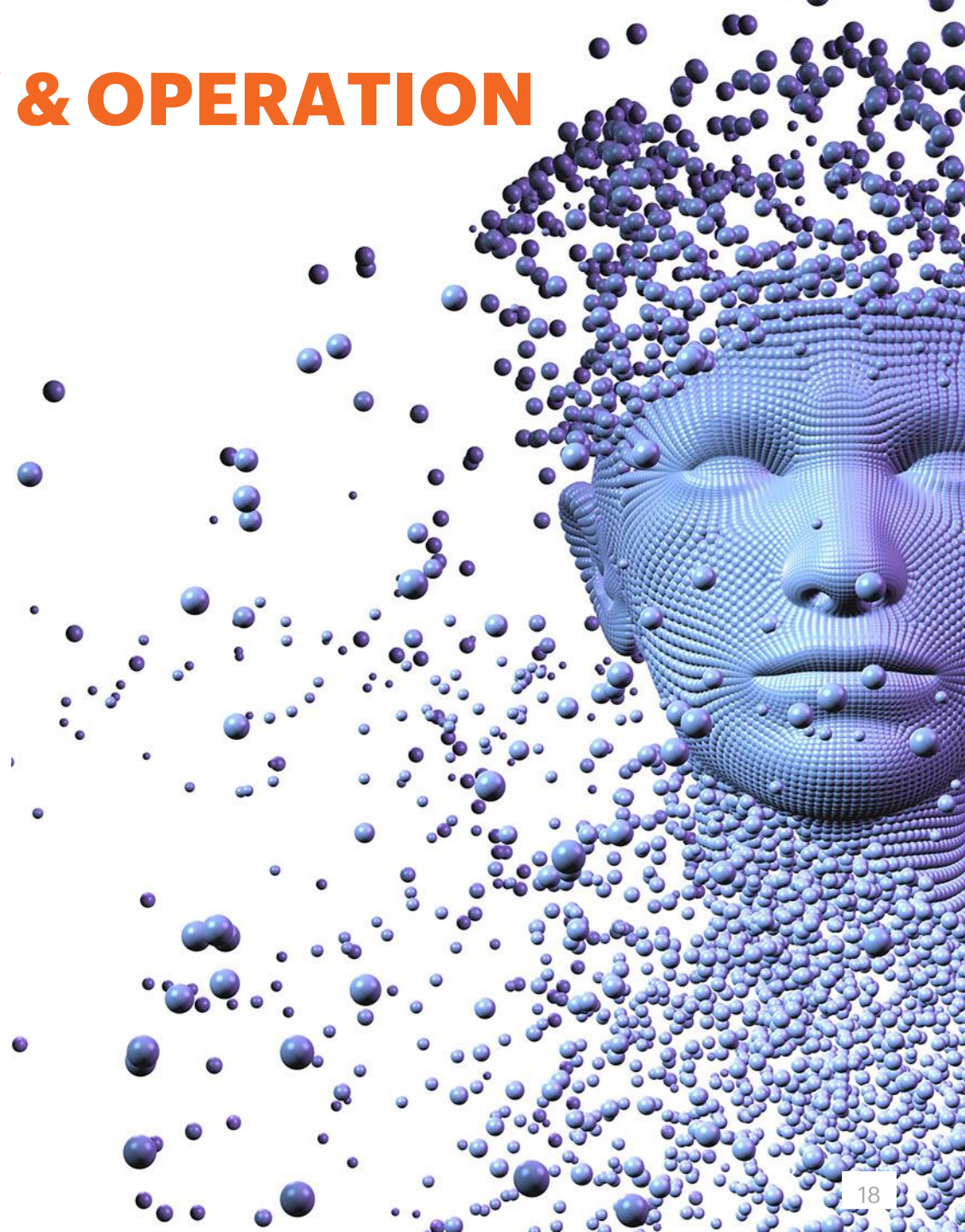
- Spear phishing campaign
- Hacktivist personas
- Social media bots
- Imagery board: 4chan



CASE STUDY: ENDLESS MAYFLY & OPERATION NEWSCASTER

SKATE

- 1. Used typo-squatted domains to create inauthentic websites**
- 2. Promoted these domains on social media platforms using inauthentic personas**
- 3. Hosted malicious mobile applications**
- 4. Leveraged “ephemeral disinformation”
– Burn After Reading**

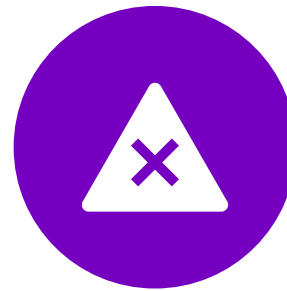


CASE STUDY: CYBER-NATIONALISM TO FANDOM NATIONALISM

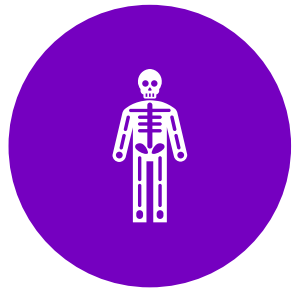
Cyber-nationalism



Born with
nationalistic and
patriotic
sentiment



State-influenced



“Striking-back”
principle: “we will
not attack unless
we are attacked”



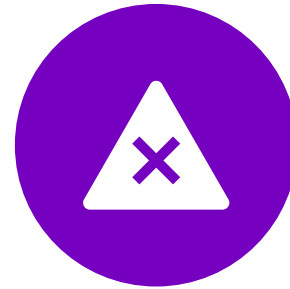
Following key
historical dates
and international
events involving
in state’s
interests

CASE STUDY: CYBER-NATIONALISM TO FANDOM NATIONALISM

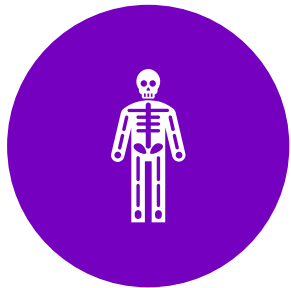
Fandom Nationalism



Born with
nationalistic and
patriotic
sentiment



State-influenced



**“Striking-back”
through social
media**



Following
international events
involving in state's
interests

CASE STUDY: CYBER-NATIONALISM TO FANDOM NATIONALISM

Diba Expedition



Actor:
Warriors/Crusaders



Weapon:
Emoji packs



Battlefield:
Social media
platforms



Goal:
National unity?

WHERE IS THIS HEADING?

HACKING



CC-BY MakeHackVoid / devdsp

[This Photo](#) by Unknown Author is licensed under [CC BY](#)



[This Photo](#) by Unknown Author is licensed under [CC BY](#) 23

A FOREVER WAR OF DECEPTION: DEEPFAKES EMERGE



SUGGESTIONS



- **Follow** geopolitical events
- **Set** social media policies
- **Filter** inauthentic accounts
- **Verify** claims
- **Investigate** information sources

accenturesecurity