black hat®
ASIA 2025

APRIL 3-4, 2025
BRIEFINGS

Weaponized Deception: Lessons from Indonesia's *Muslim Cyber Army*
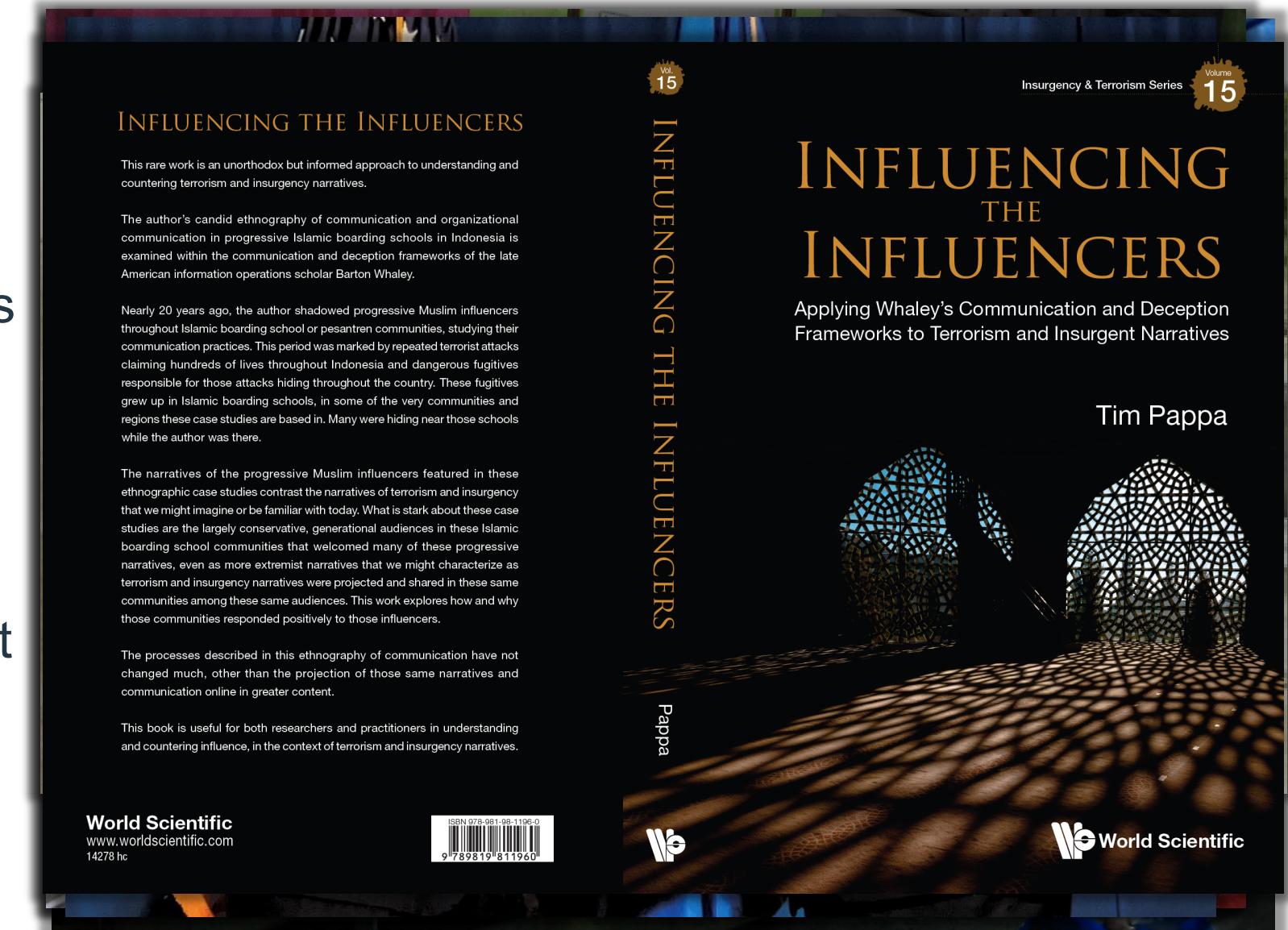
Tim Pappa

From Islamic boarding schools...to the FBI's '*Criminal Minds*'

I lived in Islamic boarding schools in 2005/2006, shadowing proselytizers and studying communication practices

I continued to analyze these communities and personalities in the intelligence community

I explored how personalities in these communities transitioned to online influence, as an FBI cyberterrorism agent and an FBI cyber profiler

INFLUENCING THE INFLUENCERS

This rare work is an unorthodox but informed approach to understanding and countering terrorism and insurgency narratives.

The author's candid ethnography of communication and organizational communication in progressive Islamic boarding schools in Indonesia is examined within the communication and deception frameworks of the late American information operations scholar Barton Whaley.

Nearly 20 years ago, the author shadowed progressive Muslim influencers throughout Islamic boarding school or pesantren communities, studying their communication practices. This period was marked by repeated terrorist attacks claiming hundreds of lives throughout Indonesia and dangerous fugitives responsible for those attacks hiding throughout the country. These fugitives grew up in Islamic boarding schools, in some of the very communities and regions these case studies are based in. Many were hiding near those schools while the author was there.

The narratives of the progressive Muslim influencers featured in these ethnographic case studies contrast the narratives of terrorism and insurgency that we might imagine or be familiar with today. What is stark about these case studies are the largely conservative, generational audiences in these Islamic boarding school communities that welcomed many of these progressive narratives, even as more extremist narratives that we might characterize as terrorism and insurgency narratives were projected and shared in these same communities among these same audiences. This work explores how and why those communities responded positively to those influencers.

The processes described in this ethnography of communication have not changed much, other than the projection of those same narratives and communication online in greater content.

This book is useful for both researchers and practitioners in understanding and countering influence, in the context of terrorism and insurgency narratives.

Insurgency & Terrorism Series Vol. 15

INFLUENCING THE INFLUENCERS

INFLUENCING THE INFLUENCERS

Applying Whaley's Communication and Deception Frameworks to Terrorism and Insurgent Narratives

Tim Pappa

Pappa

World Scientific
www.worldscientific.com
14278 hc

ISBN 978-981-98-1196-0
9 789819 811960

World Scientific

What Did *Muslim Cyber Army* Do?

They inflamed religious and political tensions with emotional angering content

They prompted misinformation, but mostly spread disinformation

They prompted violence

They were "traitors" to Indonesia

"Why do you care about Muslim Cyber Army? They are no longer a threat"

Seputar Muslim Cyber Army: sebarkan isu PKI bangkit,

President Jokowi: Thoroughly Investigate Muslim Cyber Army! - iNews Afternoon 06/03
3.9K views • 6 years ago

Official iNews

Air Date: 06/03/18 A daily news program that presents the fastest and most up-to-date information in detail from various ...

Wiranto: The Muslim Cyber Army is a Traitor to the Nation
6.5K views • 6 years ago

NewsSatu

Coordinating Minister for Politics and Legal Affairs Wiranto emphasized that the parties involved in the **Muslim Cyber Army** (MCA) are traitors to the nation. Wiranto ...

Dugaan keterkaitan kelompok MCA dengan kelompok Saracen, menurut polisi, didasarkan pendalaman di media sosial.

Who Did *Muslim Cyber Army* Target?

Islamic boarding school (*pesantren*) communities mostly throughout Java, Indonesia

Many MCA members grew up in and lived in these same communities

Think of electoral seasons in your own countries

What Have I Learned About *Muslim Cyber Army?*

The threat of MCA was a "memetic" response to LGBTQ and political content

Most Admins never met in person until prison

There is limited public evidence of CNA/CNO, despite repeated media claims of MCA "*snipers*"

There were some organized functions and some people guiding some of those functions, but much of this was coordinated and organic trolling

Their origins are still unclear

What Else Did I Discover About *Muslim Cyber Army?*

One of the main Admins was a middle-aged divorced single mother of four children

Tara Arsih Wijayani is dead

Tara appeared to be very different than how the news media and her "neighbors" characterized her

While deception is rarely mentioned, MCA demonstrated every established deception technique in the Bell-Whaley deception framework

Tara was a leading Admin in "MCA Family" who likely had significant influence over MCA deception techniques

Idealized Self: Tara Arsih Wijayani

Responsible

Ebullient

Secure

Distinguishable

Magical

Soulful
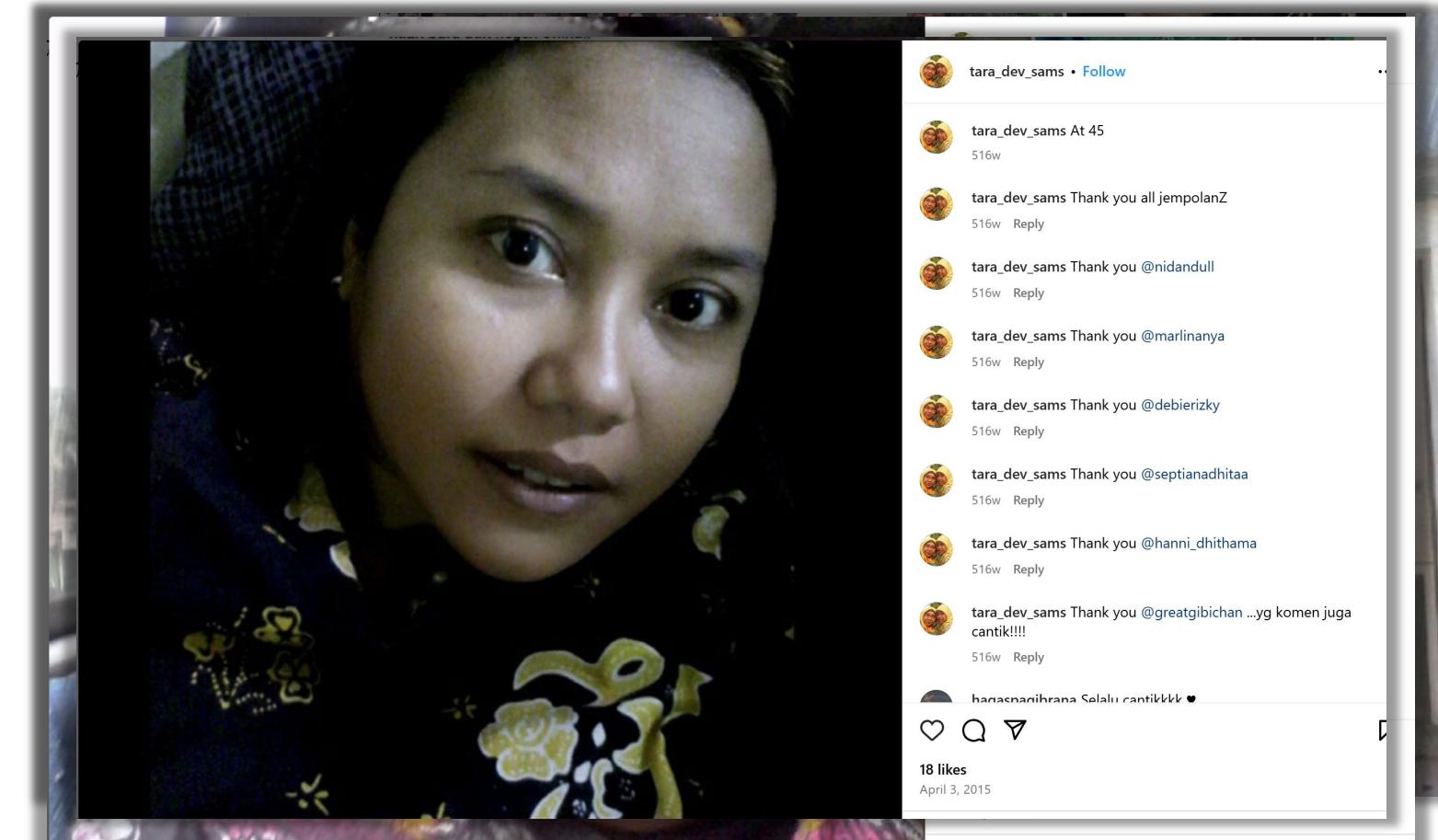
Self Actualization: Tara Arsih Wijayani

Her move as a teenager from Jakarta to Yogyakarta appeared to be positive

How did she Make Meaning from her marriage and divorce?

Are her children from a previous marriage or relationship?
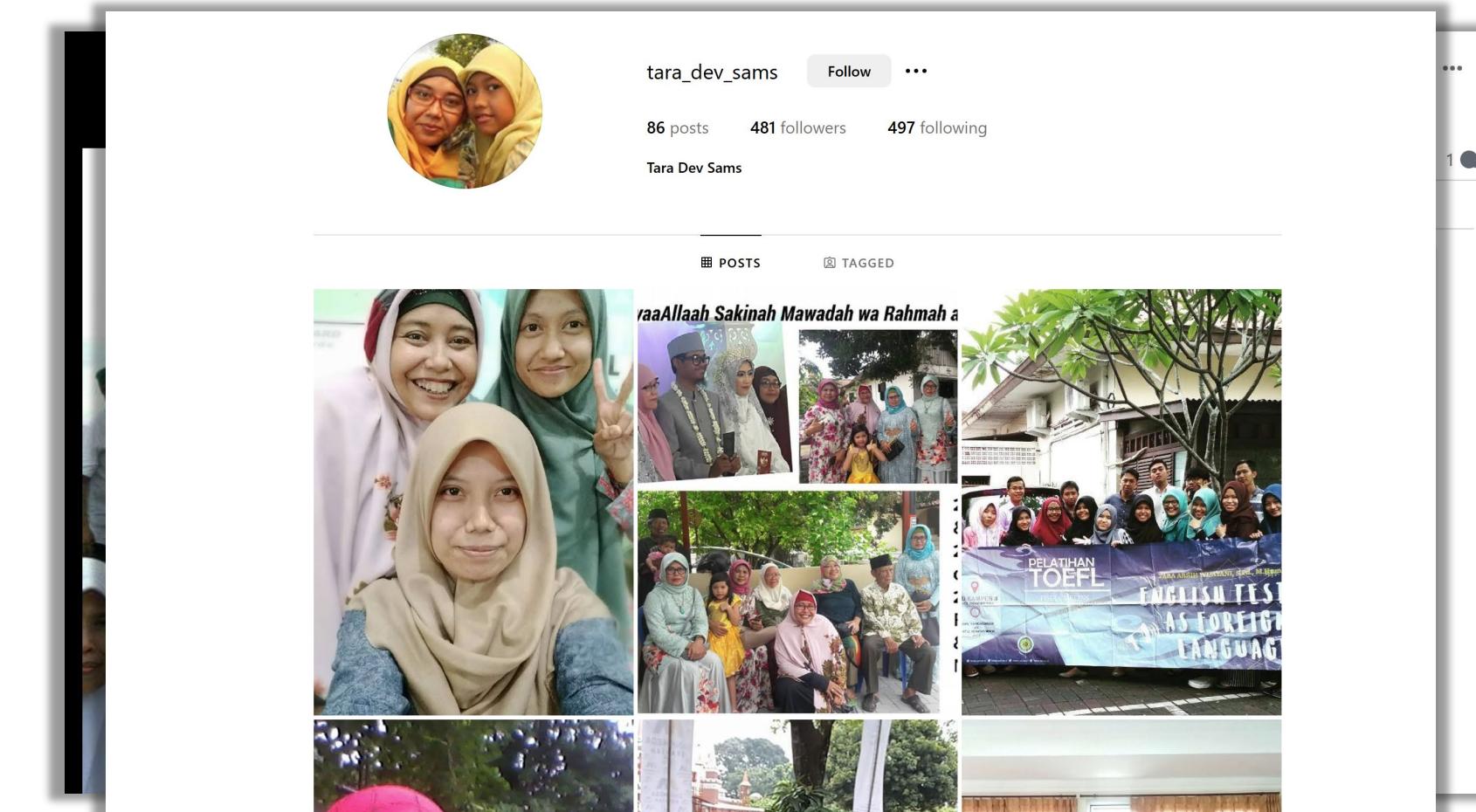
Was her role and experiences in MCA her version of "edgework"?

Identities and Roles: Tara Arsih Wijayani

"…even great love must keep its flame alive"

"…cinta besarpun harus dijaga nyalanya"
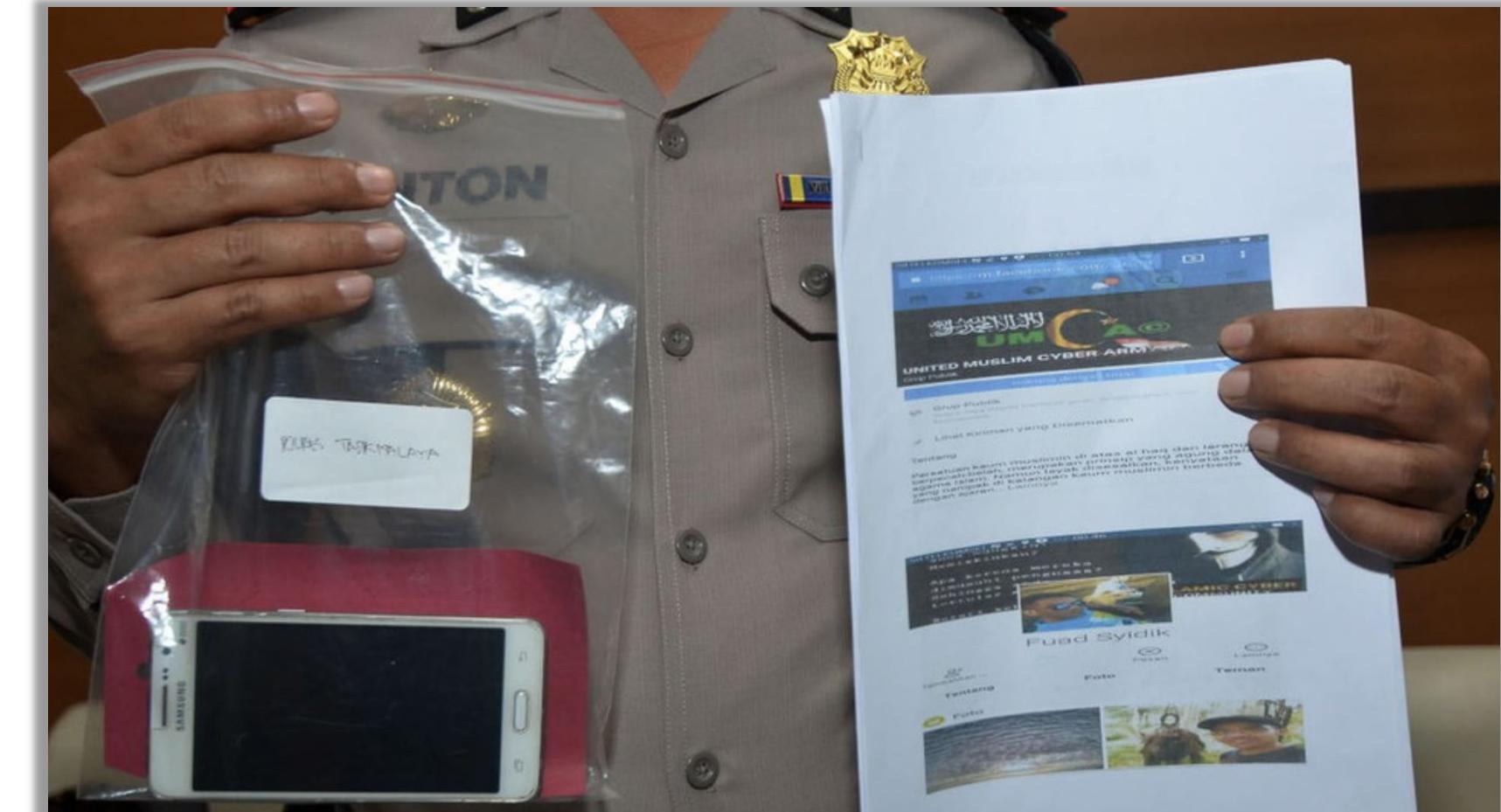
How Tara and *Muslim Cyber Army* Demonstrated Cyber Deception Techniques

What makes MCA techniques different than trolling and making 'fake news'?

People use deception to distort someone's decision making

Examples of the authentic cultural and social media *richness* of MCA's cyber deception approaches and content

Outlining MCA techniques within a Bell-Whaley deception framework can reveal how that deception technique is effective
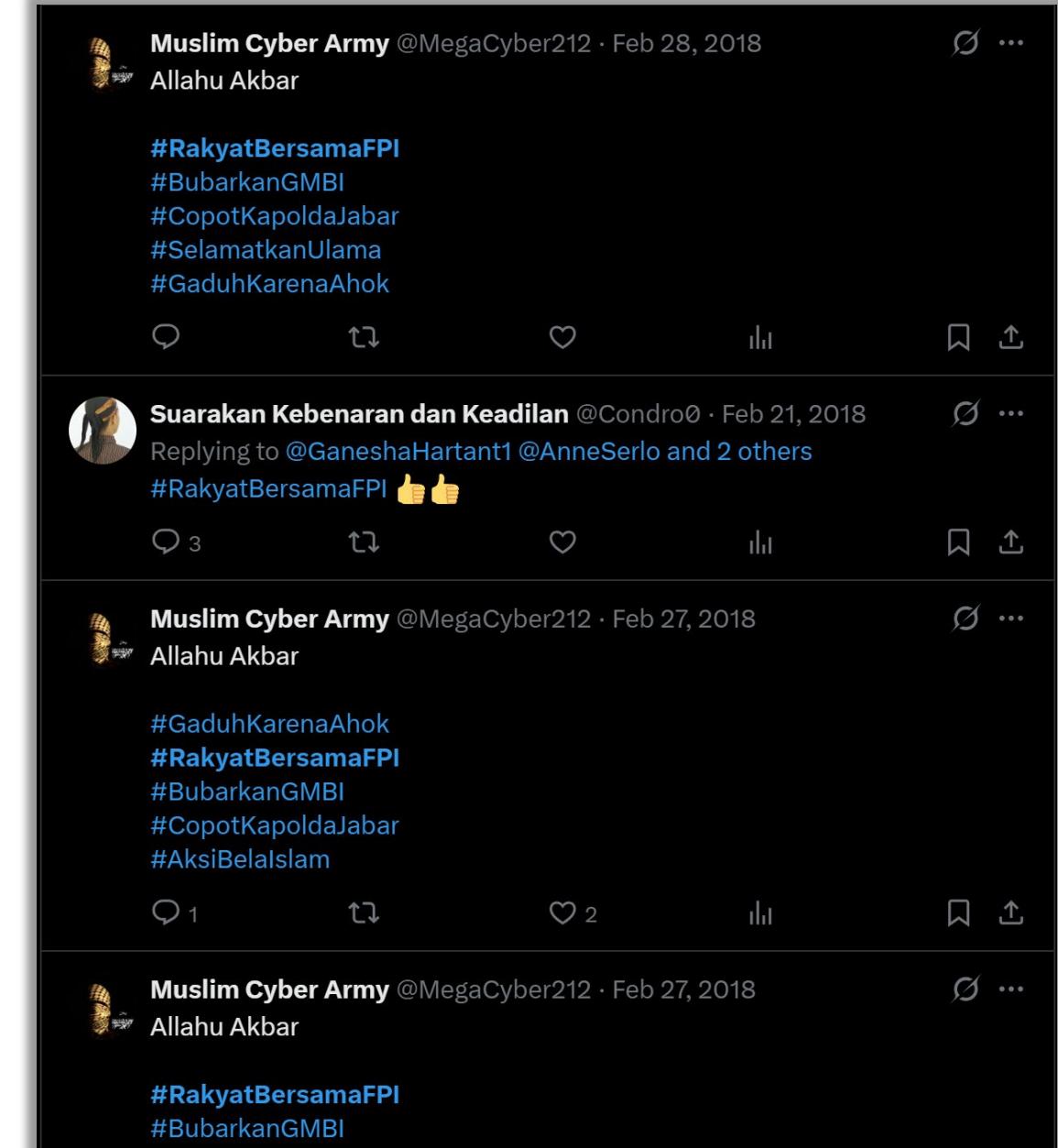
Dissimulation: Masking

Hiding the real by making it invisible

MCA admins and other organized personalities generally managed dozens of accounts that resembled everyday people and narratives from these communities

MCA mixed their controlled accounts and created or repurposed content in these threads

MCA admins reported accounts and personalities to Facebook and other platforms alleging violations of service

Dissimulation: Repackaging

Hiding the real by disguising

MCA admins formed Facebook groups for selective resharing of news

Thousands to hundreds of thousands of people subscribed to or followed these "news" accounts

MCA admin-controlled accounts were tagged on less inflammatory content, such as posts about character building in *pesantren*. Those accounts reshared the same content with more inflammatory content.
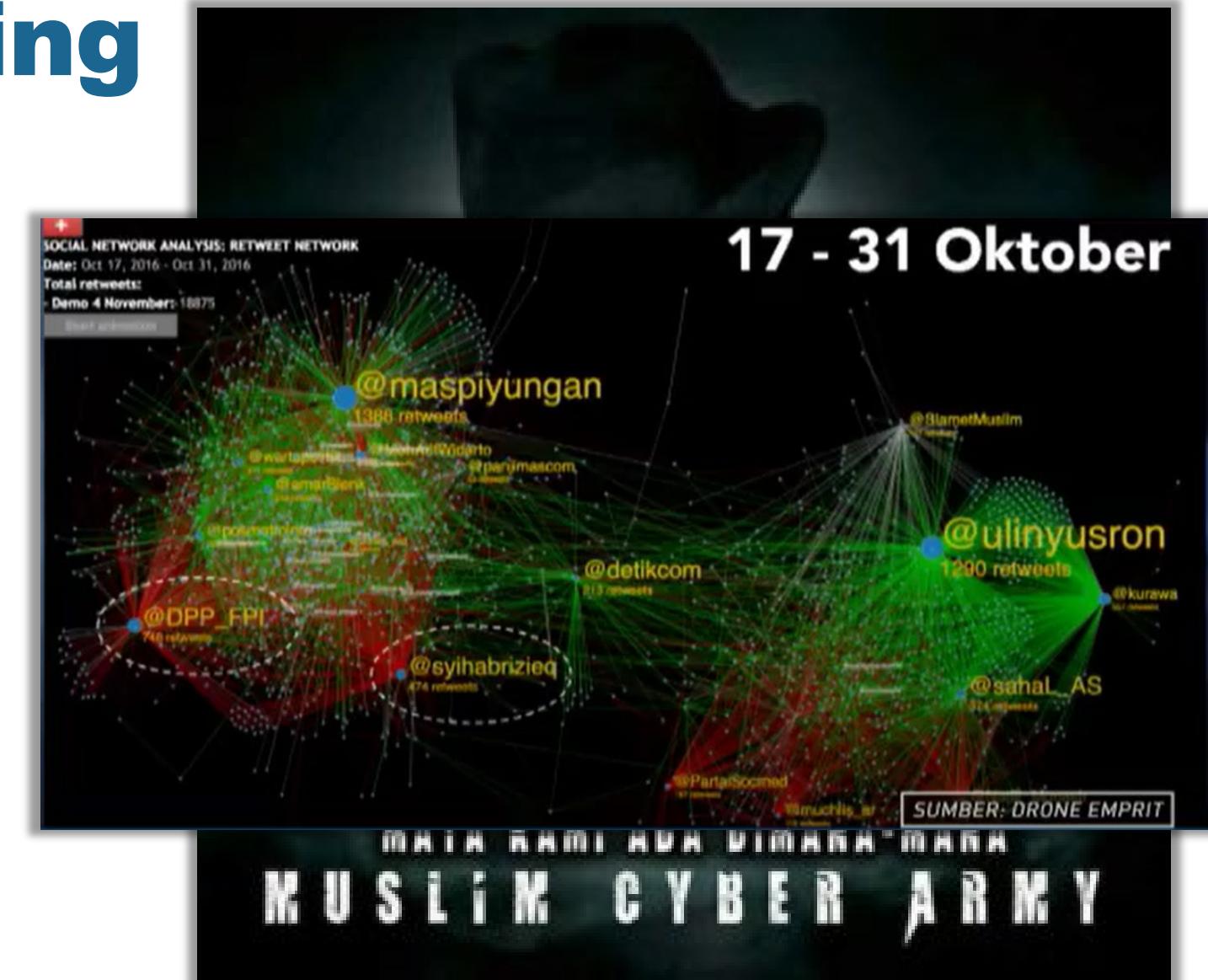
Dissimulation: Dazzling

Hiding the real by confusing or enticing

MCA admins generally planned "attacks" with their "snipers" twice a day, which involved staging and reporting inflammatory exchanges with target personalities or masquerading as these target personalities to get them banned

MCA projected mixed imagery often of Anonymous and Islamist hacktivist references and cues

MCA controlled activity was often projected exponentially by the broader target public
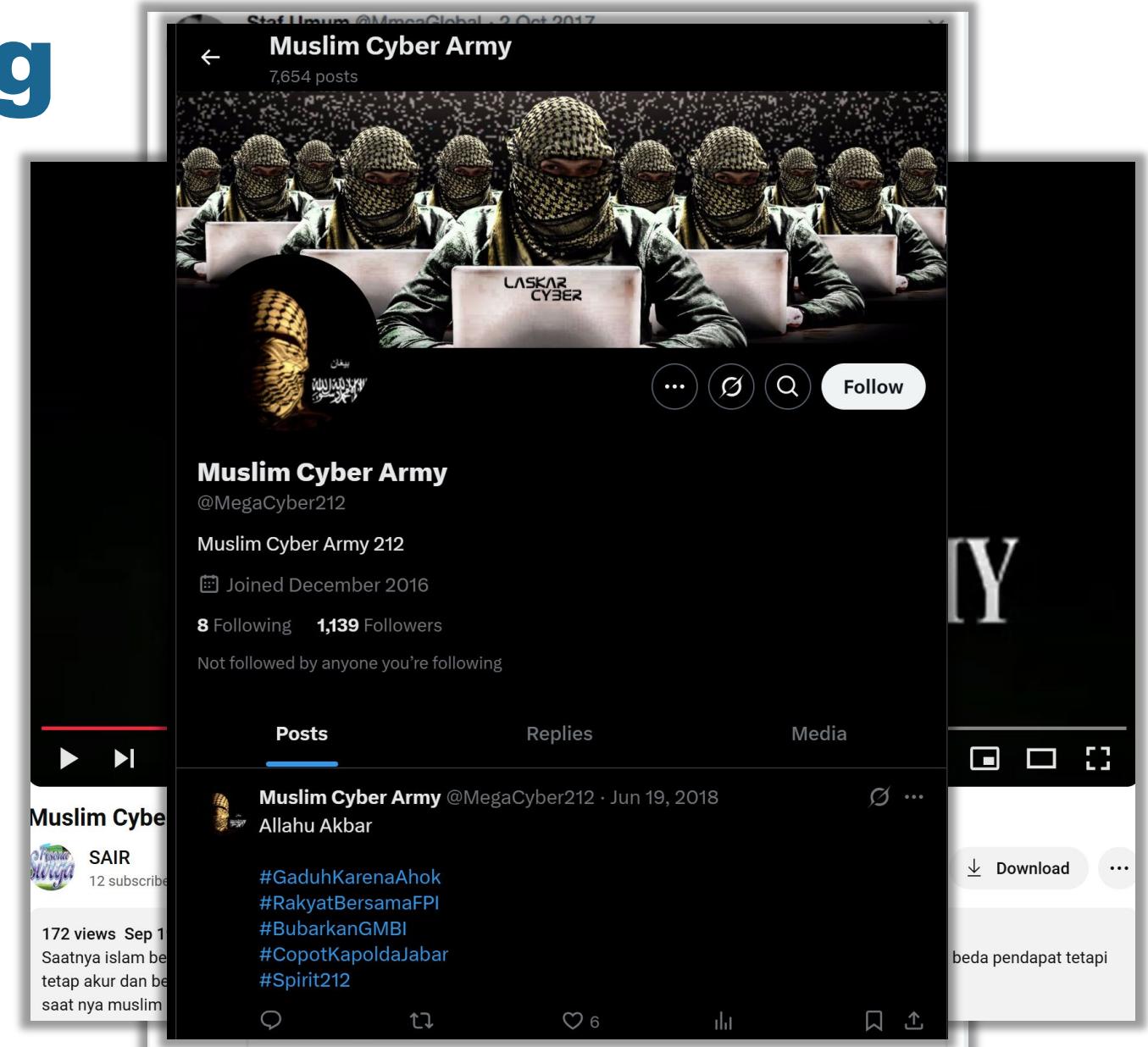
Simulation: Mimicking

Show the false by imitating

MCA controlled bots boosted content sharing and displayed what appeared to be public accounts from these communities

"Muslim Cyber Army" has been used in variation by all kinds of online personalities, from Islamist hacktivists to cyberterrorists to cybercriminals to teens having fun

MCA admins deny involvement with Anonymous or Saracen, but their language and myth- or folklore-making is similar
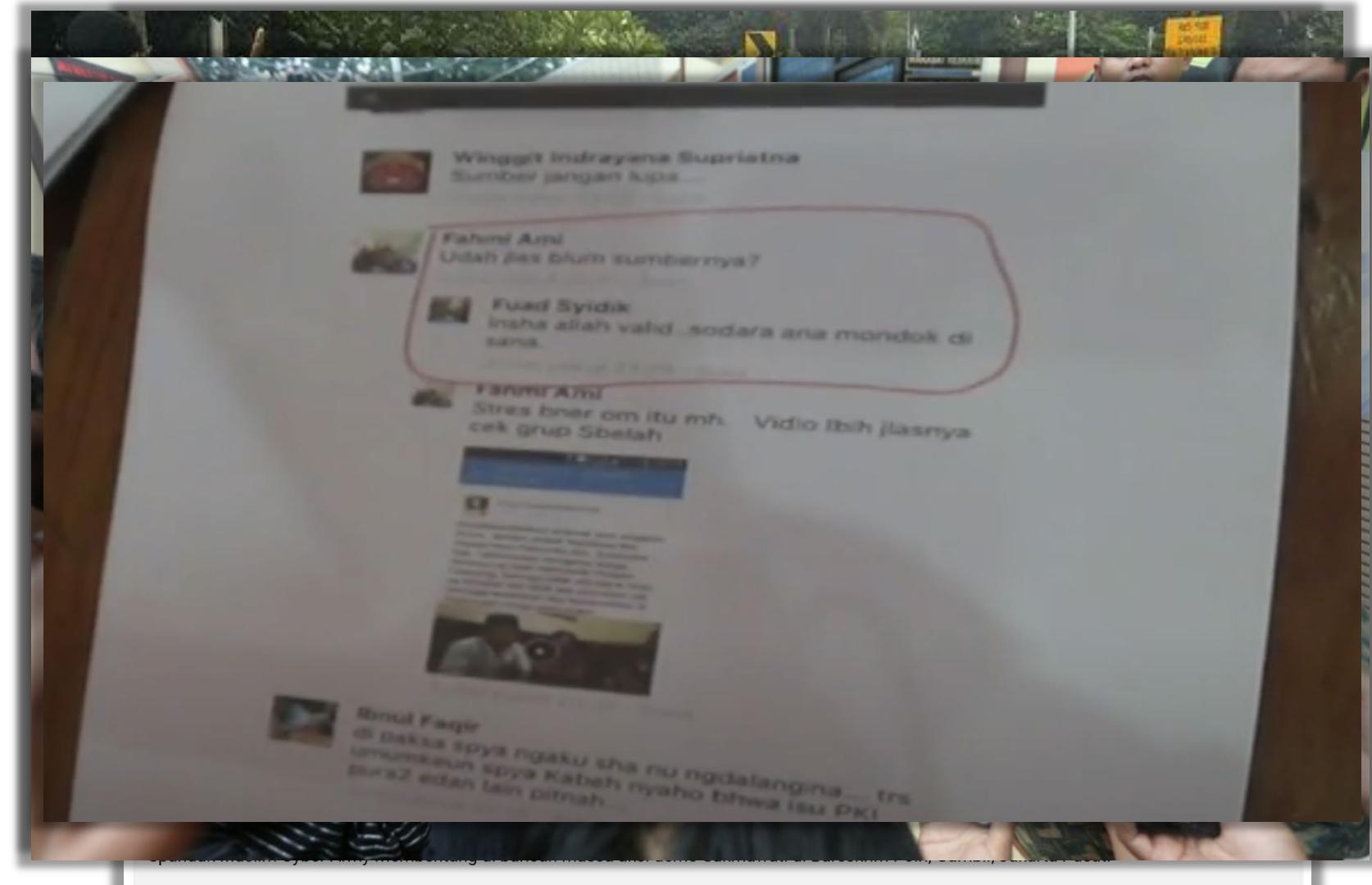
Simulation: Inventing

Showing the false by fabricating

MCA invented its role in broader movements and "political imagination"

MCA likely influenced real and imagined perceptions of affiliations or relationships with organizations

"We are…"

Inventing was simple online, because it reflected broader attitudes and emotions
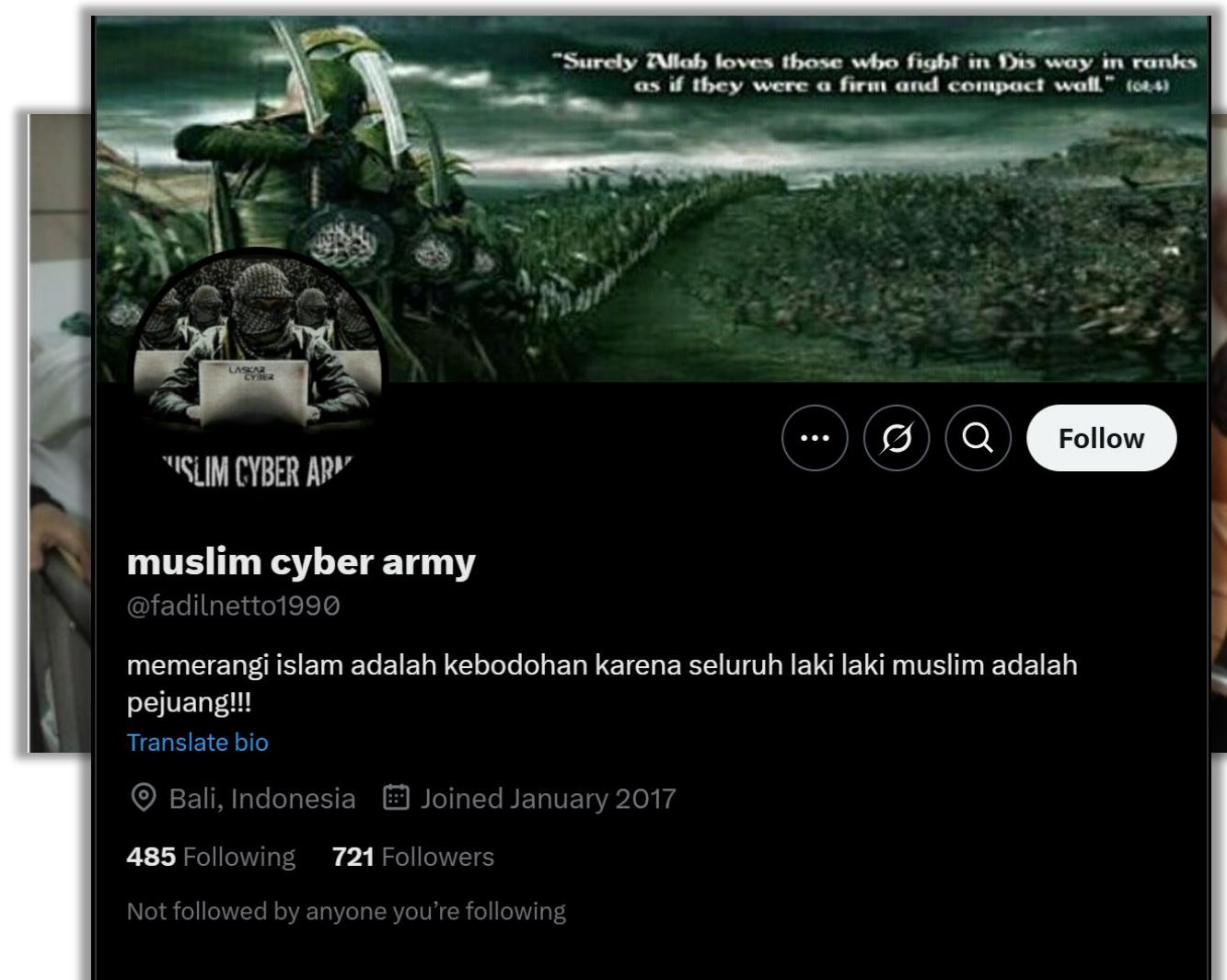
Simulation: Decoying

Showing the false by masquerading

MCA and other online personalities would repurpose content or create content suggesting *kyai* were being harassed or attacked by non-Muslims

The content and storylines resembled real but rare events

Accounts related to MCA or controlled by MCA admins generally appeared to resemble Islamist hacktivist account imagery and narratives

"Surely Allah loves those who fight in Dis way in ranks as if they were a firm and compact wall." (61:4)

MUSLIM CYBER ARMY

muslim cyber army
@fadilnetto1990

memerangi islam adalah kebodohan karena seluruh laki laki muslim adalah pejuang!!!
Translate bio

📍 Bali, Indonesia   📅 Joined January 2017

485 Following   **721** Followers

Not followed by anyone you're following
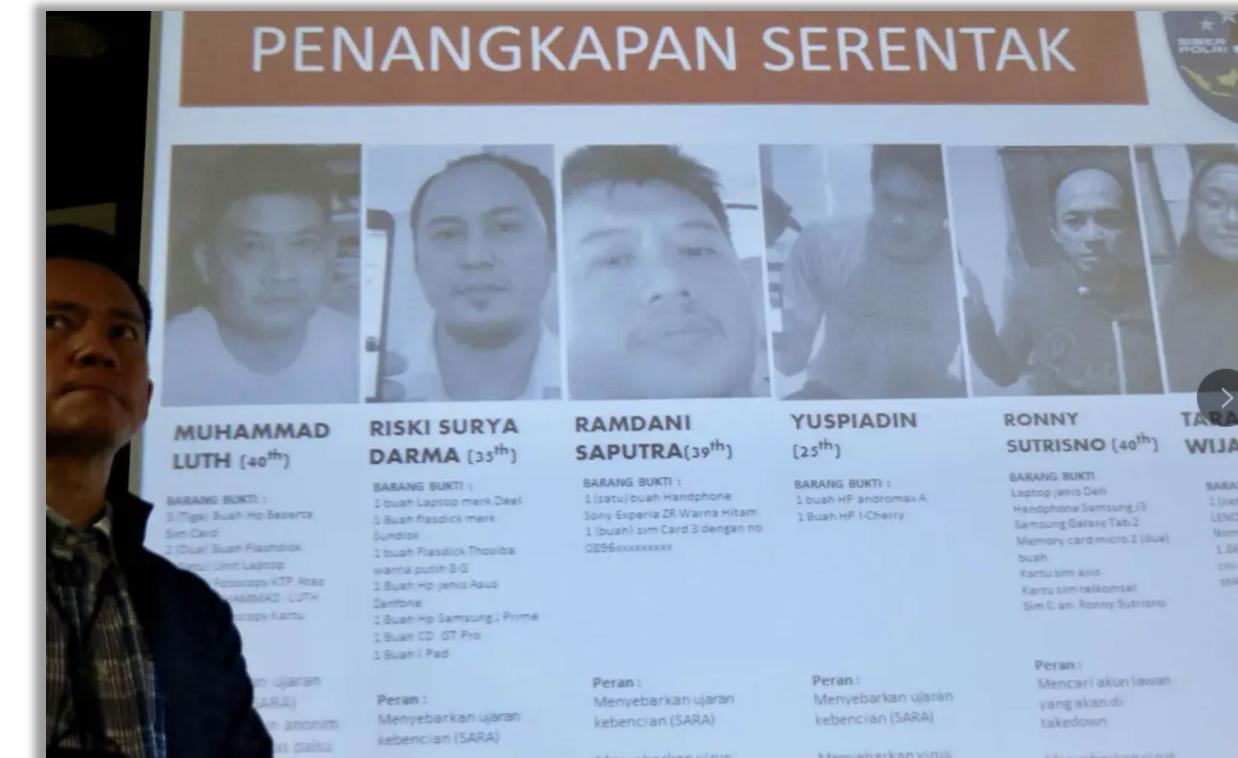
What Did *Muslim Cyber Army* Contribute to CTI Practices and Research?

We should look for more examples outside of Russia that demonstrate how governments and the news media have mischaracterized threat actor capabilities and reputation.

Even generic names like *Muslim Cyber Army* often reflect deeper social attitudes.

Threat actor collectives can be dramatically disruptive and effective, even without many tools or limited capabilities. A cyber deception framework can reveal some of those alternative techniques.

The interpersonal relationships and personal lives of threat actors provide the best insight into motivation. Incorporate behavioral analysis into your CTI.

What Did *Muslim Cyber Army* Contribute to the Cyber Deception Practices and Research?

Demonstration of manipulated content delivery within deceptive storylines, in dynamic environments.

Demonstration of effective cyber deception application, with perhaps limited to no backgrounds in deception training or practice.

Cyber deception techniques became a force multiplier, resembling what we commonly associate with nation state enterprises capabilities and resources today.

Reexamine current and historical case studies of hacktivist and broader cybercriminal activity with a cyber deception framework for more insight on techniques without tools.