LikeWar: The Weaponization of Social Media

Peter Singer, Author
Emerson Brooking, Author

Kathleen H. Hicks, Senior Vice President, CSIS
Center for Strategic and International Studies

October 5, 2018 1:30 pm - 2:30 pm

https://www.csis.org/events/likewar-weaponization-social-media
LikeWar: The Weaponization of Social Media
Center for Strategic and International Studies

• Where did the title, LikeWar, come from? What brought this book idea together?

• LikeWar is how social media has changed news, politics and war and in turn, how news, politics and war have changed the Internet

• If cyber war is about the hacking of networks, LikeWar is about hacking the people on the network by driving ideas viral through a mix of likes but also lies and the system’s own algorithms

• LikeWar reflects how war & politics come together (Clauswitz - politics by other means)
  • Competing and even self-identified online armies use the same tactics to accomplish their real-world goals
  • Examples: #resistance versus the alt right, ISIS versus the U.S. military coalition, Kanye West fans versus Taylor Swift fans – same tactics (doctrine) to win the war online
Events that prompted the genesis of this book:

- The idea of a military member in a conflict zone finding a declared enemy on social media - possible after DOD relaxed social media guidelines
- 2013 Westgate Mall attack in Kenya – attack was live-tweeted by the terrorists – because Kenyan authorities were slow in response, al Shabaab ran the narrative for a time
- 2012 – IDF eight-day air campaign against Hamas – not kinetically significant but it is described as the first Twitter war because 10 million tweets were exchanged by online proxies on both sides to shape public opinions
- 2014 – ISIS use of social media because their use became the focus of the U.S. political class and everyday Americans
- 2014 – ISIS execution of James Foley in a viral video – Americans reportedly more afraid after this video than post-9/11 time period
- 2016 – same phenomena that focused on terrorism could also be applied to modern politics - elections
- 2017 – Charlottesville riots with white nationalists – gathering possible with online help
LikeWar: The Weaponization of Social Media
Center for Strategic and International Studies

- Transparency – even the most secretive operation cannot stay hidden for long
- Contrast the D-Day landings and the UBL operation
  - D-Day - two-year mobilization in the British Isles with 40 million tons of supplies, and one million soldiers – Germans knew that it is coming but not *where* until the day
  - UBL Raid in 2011 – nobody knew until the day of the raid - live-tweeted by a Pakistani IT consultant – once the event was identified, it took a few minutes for American journalists to corroborate - a new source of information - the raid would never have been observed before – 2011, about 6% of Pakistanis were online and now about 25% online
- Social media mix is chronic over-sharers and information that doesn’t disappear but accumulates – bits used anytime by actors that don’t have our best interests at heart
  - Chinese citizens rely on mobile apps – the CCP is moving to score every citizen based on their online habits and also a social credit score of other people in their peer group – an indirect and effective social engineering approach
Examples of secrets of evil deeds that can now be found by people who are fundamentally new to the game

- Malaysian airplane shot down over Ukraine – a citizen-investigator group pieced together open source information to document Russia’s role in the shoot down
  - Identified the truth - that truth was also buried in many alternate theories – the truth is out there but it is heavily buried
- Same group also pieced together who poisoned the Russian living in England
- Mike Flynn, in interview, spoke how the sweeping change of the Internet affected his military career as he entered a political campaign – he understood how to place multiple bits of information and then watch the information grow
• **What are the winning strategies?**

• Social media is the nervous system of the modern world and a battleground
  
  • A set of tactics have emerged that disparate groups keep crystallizing towards winning on the web or driving their message viral

  • The power of narrative or storytelling

  • Example: Spencer Pratt who started as a producer and created *the Kardashians* – then became a reality actor on *The Hills* – in an interview, Pratt and his wife spoke of how they achieved their goals through narrative and discussed how he manipulated the media and how to get what you want – *We are all reality stars now but everyone is just as fake as we were*

• State Department team who worked the counter-ISIS program were interviewed – authors quickly found that Spencer and Heidi *got it* but the State Department team *did not* – narrative
LikeWar: The Weaponization of Social Media
Center for Strategic and International Studies

- Planned authenticity

- Taylor Swift and Junaid Hussain example - in interview, Swift talked how originally, it was Myspace, and then Instagram

- Junaid Hussain was a failed British rapper who radicalized, joined ISIS, became the head of ISIS cyber operations and rose to the top tier of ISIS

- Both reached down to directly engage with their fans – it really is Taylor Swift and Junaid Hussain who congratulate fans individually with the full knowledge that the world is watching

  - Achieved a double-goal which is what is so different about this technology

    - Mass-scale broadcasts
    - Immediate one-on-one interaction
• Positive consequences – Arab Spring example

• Negative consequences

  • The Russian democratic uprising, Putin looked at it as the most significant challenge to his authority and as an attack from the West through social media

  • The origin of the modern Russian information strategy to find fissures in American society and exacerbate them, to seed tens of thousands of fake accounts across Twitter, to masquerade as socially inflammatory personalities on Facebook so Russian propaganda would reach 140 million Americans

• Collision between online and real world was such that the Russians could plan an event from Russia, use sock-puppet proxies, and have hundreds of Americans turn out to protest one thing or the other – could organize a protest and counter-protest so Americans turned out to protest each other

• Lone wolf and remote control – use social media very effectively against Americans
Physical Battlefield Effect

• Battle of Mosul and the ISIS win – with the old rules, ISIS should not have won as ISIS had 2,500 against 20,000 defenders

  • ISIS engaged in a fundamentally different way by weaving together a new communications technology – rather than try to keep its invasion a secret, it wanted the world to know about it and created a hashtag (#AllEyesOnISIS) and included sock puppets (a web persona with a real person behind it), bots (a web persona with a machine behind it) – contrast with trolls who are trying to provoke an emotional response

• ISIS pushed their message ahead of their force which spread the contagion of fear, much like the radio was used in the 1940s – Iraqi soldiers saw scenes of battlefield loss and soldiers killed – the world saw ISIS’s messaging with no rebuttal

• A victory online before the physical battle – the Iraqi Army essentially melts away

• Second battle for Mosul – the U.S./Iraqi force learned and used the same strategies and tactics and weaved them into battlefield operations
LikeWar: The Weaponization of Social Media  
Center for Strategic and International Studies

• Hacking networks and which nation has the best cyber defense - probably North Korea and not because they have the best talent or the best organization but a combination of an authoritarian regime and as many internet connections as a Manhattan city block

  • Their trade-off is a bad economy and no freedom

• Similarly, the Internet is balkanized by social media – very different experiences from people in different places based on market differences and what the government is willing to do

• Turkey, a retweet equals an endorsement – a Turkish man retweeted and sent to prison

• China uses technology to screen and a perverse incentive system (a social reading)

• For the U.S. – don’t become authoritarian and don’t stop using social media

  • Understand the new rules of the game and adjust for them

  • The U.S. has become the nation that others point to and say, don’t let what happened to them, happen to us, in defense circles - understand this new type of threat space
• How should government and industry interact with each other?

• Not a task that Silicon Valley wanted so they avoided it for many years

• Silicon Valley thought information was a market place for ideas and the best ideas would rise to the top

• A moment of reckoning - after the 2016 election where social media platforms had been the primary driver of American voting patterns and an invisible battlefield for Russian influence operations – this reckoning played out in stages similar to the stages of grief

• The best thing to do:
  • Invest more time and money in content moderation policies and in understanding that they should be carefully attuned to the information that flows through their systems
  • Be aware that social media services are being exploited by non-state groups and international adversaries that mean America harm
LikeWar: The Weaponization of Social Media
Center for Strategic and International Studies

- Like cyber security, it is not only government having a role but government, industry, and the individual
  - Within government, many portions of government and not just DoD
- Responsibilities include changing our concepts of the threats, reorganization, modeling from other nations, new training, new organizations, perhaps reinvent things from the Cold War (active measures working group which worked against incoming KGB operations across the developing world)
- Election security - how to frame it in Hollywood, think tanks, media or government?
  - Focus on hacking a voting machine, though a real risk, has never been done at a national level but hacking a voter has been done on a national scale with indications that it will occur in 2018 election cycle and beyond
Question and Answers

Q – SECDEF established information as the seventh joint function - how to organize as a staff function? How to best exercise for combatant commands?

A – A parallel in history – with the Blitzkrieg (tanks, planes and radios together), the American military response was things like Fort Polk’s *Louisiana maneuvers* (*how to we shift from horses to mechanization*) – includes everything from doctrine to learning tactics to experience

A – After 9/11, we built fake villages to learn a newer warfare

A – Now, we build fake internets over fake battlefields to learn a newer warfare – some learning from Estonia, the IDF, the British 77th brigade and others along with the Russians and Chinese

A – Do not gear up to fight the last war – certain truths will remain - consider what will artificial intelligence bring to the space
Q – Expand on *planned authenticity*

**A** – Power in being *real* – the more *real* a thing is, the more it will win – Aristotle on democracy, A person who can persuade others that he/she is better and also *of them*

- To do this, use the technology of the day (*born in a log cabin*, politicians visiting New Hampshire diners, President Trump’s use of social media combined his personality and his early addiction to the space – then, Trump as business leader was getting into shouting arguments online and before the world - gave him attention – an early adopter

**A** – ISIS was comprised of millennials that put out short, quick, and snappy responses versus Al Qaeda’s (a group made up of the prior generation) long-winded sermons - ISIS was competing against Al Qaeda first – now, AQ messaging is short and snappy – the Taliban has evolved as in 2001, social media did not exist and now, it is the portal to observe the war - before, the U.S. military and the Taliban did not talk to one another and now they do via social media – constant communication in front of the world
A – Inundation with low-cost experimentation

- Refine *by volume* like never before with *live focus-group* testing of 10,000s to 100,000s iterations for one message over Facebook, within a political context

- Compare to traditional focus-group testing, all those costs are gone

- Like aerial carpet bombing and precision munitions with immediate feedback

- With the Trump *campaign*, Twitter won him the news cycle but Facebook won him the election – a strategy of inundation with experimentation
Q – Neural networks and their impact?

A – Most people could tell the story of Benjamin Franklin or Thomas Jefferson but most could not tell the story of the first social network that was on ARPANET for scientists to collaborate

• One scientist sent out a group email to ask, “What is your favorite science fiction?” – the very first social network was people talking about science fiction and then, the best restaurants, the best whiskey – out of these observations, “I just created something social”

A – Now, neural nets or machine learning is applied to create hyper-realistic and false voices online – done to improve marketing and also weaponized – now, bots are not very realistic but are very effective – one third of Brexit conversation was generated by artificial voices – the U.S. and Mexican elections were one third or more – the automated voices are much more real now than in past elections
A – traditional work is linear - neural networks are fascinating as they are endless and tuning them doesn’t necessarily allow how they work since there are millions of input and millions of output – they can create novel ideas and original construction

• Applied to disinformation, now a profile picture can be checked by running a Google image reverse-search to find that it is a stock image but that won’t be the case with new and original images being produced by neural networks (also video and audio)

A – These technologies producing deep fakes will be definitively weaponized and have a greater effect on the U.S. military and the American political system than many weapons and threats that we obsess over – we worry now about EMP (electromagnetic pulses) but deep fakes will have more of an impact – a hyper realistic report of a war crime or a President’s speech as examples – when something is real, people may not believe it

A – U.S. will have to develop counters to this just like we would with any other weapon and how to rapidly identify these types of technologies

• Create markers that make it harder for these items to work and more