Manipulating Fast, and Slow.

Dr Mary Aiken

> "*Today's technology is such that the final address can be masked and camouflaged to an extent that no one will be able to understand the origin of that address. And, vice versa,* ***it is possible to set up any entity or any individual that everyone will think that they are the exact source of that attack.*** *Modern technology is very sophisticated and subtle and allows this to be done. And when we realize that we will get rid of all the illusions*"[1]
>
> President Vladimir Putin June 2017

I agree, unreservedly, attribution is highly complex in cyber contexts – and therein lies the problem. Illusion is interesting, pertaining to "an instance of a wrong or misinterpreted perception of sensory experience."[2] This curious word choice speaks to the core of the problem space, that is, the recognition of the cyber domain as an experiential environment, one whereby our human senses finely honed in the real-world may fail us – and importantly where investigative processes may also stall, or fail.

As a discipline, cyberpsychology focuses on the impact of emerging technologies on human behavior. Although scientifically the primary emphasis is on Internet psychology, other technologies are also incorporated; virtual environments, artificial intelligence, gaming, digital convergence, connected devices and mobile technologies. Cyberpsychology is rapidly developing into an established field within applied psychology and is expected to grow exponentially due to the continuous evolution of digital technologies, and the unprecedentedly pervasive and profound impact of the Internet on human beings.

Online and offline behaviors can be very different, but are nonetheless connected:

> "Claims for the independence of cyberspace…are based on a false dichotomy …physical and virtual are not opposed; rather the virtual complicates the physical, and vice versa."[3]

This interdependent relationship between the virtual and the so-called 'real-world' means that we must now consider technology in a new way, necessitating a conscious paradigm shift to the conceptualization of cyberspace as an environment, as a place, as Cyberspace.

In the 1940's Roger Barker founder of the interdisciplinary field of ecological psychology argued that social settings influence behavior. The field was established to examine the

---

[1] https://www.memri.org/reports/st-petersburg-international-economic-forum-plenary-meeting

[2] https://en.oxforddictionaries.com/definition/illusion

[3] Slane, A. (2007). 'Democracy, social space and the Internet', *University of Toronto Law Journal, 57:* 81 - 104

relationship between psychological mechanisms and the social and physical environments in which humans operate, with a distinct emphasis on investigating human behavior in its natural state. In the 1980's environmental psychologist Harold Proshansky[4] continued to research the relationship between 'man and his physical setting' arguing that;

> "No corpus of knowledge about human behavior and experience can be complete or fully meaningful without the inclusion of concepts and principles relevant to the influence of physical settings regardless of how much or how little they contribute to the variance in such behaviour or experience."[5]

Proshansky tried to solve difficult environmental problems in the pursuit of societal well-being.

In June 2016 NATO declared Cyberspace a 'domain of warfare'[6] – acknowledging that current battles are waged not only on land, sea, and air but also on computer networks, and yet, this seismic declaration passed almost unnoticed. This pronouncement represents a significant development, an official acknowledgment that 'cyber' is an actual place. NATO's statement has implications regarding the psychology of an environment created by people, devices, connectivity and social technologies; it also has consequences for society, raising critical questions concerning policy, practice and governance in Cyberspace. Important policy issues must be considered, for example; the question of territorial jurisdiction of the International Criminal Court[7] (ICC) over international crimes against humanity and acts of aggression committed via the Internet. Over 120 countries worldwide support the ICC from the Netherlands to Cambodia, but the United States is not one of them. The ICC under the Rome Statute system has called on all countries to "join the fight against impunity"[8] so that perpetrators of widespread, systematic international crimes are punished. What does an atrocity or a systematic crime against humanity look like in Cyberspace? Is there a role for the ICC regarding international or indeed multinational criminal interference in national democratic processes? Could a next-generation ICC supported by the United States fight impunity in Cyberspace?

Cyberpsychologists maintain that human behavior can fundamentally change online. A formidable matrix of factors such as (perceived) anonymity, escalation, online disinhibition, psychological immersion, impulsivity along with 'minimization of authority'[9] dictate that people can act very differently online. We also must consider adverse effects of global connectivity, for example, a cyber effect[10] I describe as *online syndication*— the mathematics of behavior in the digital age whereby activists, cybercriminals, and extremists can find each

---

[4] Proshansky, H. M. (1987). "The field of environmental psychology: securing its future." In Handbook of Environmental Psychology, eds. D. Stokols and I. Altman. New York: John Wiley & Sons.

[5] https://www.jstor.org/stable/1084002?seq=1#page_scan_tab_contents

[6] https://www.wsj.com/articles/nato-to-recognize-cyberspace-as-new-frontier-in-defense-1465908566 [7] https://www.icc-cpi.int/about

[8] https://www.icc-cpi.int/about

[9] Suler, J. (2004). The online disinhibition effect. Journal of Cyberpsychology and Behaviour, 7, 321-326.

[10] http://www.maryaiken.com/cyber-effect/

other in few clicks under cover of anonymity and fueled by online disinhibition. Now factor in "the filter bubbles, echo chambers and feedback loops that distort and shape the information served up by search and social technologies and can profoundly impact our perceptions of the world… this becomes far more serious when the information received reinforces disturbed thinking. It's one thing to become the subject of a filter bubble that strengthens your desire to exercise, unfortunately, little thought has been given to those who may become trapped in negative feedback loops online, whereby distorted thinking or extreme beliefs may be reinforced algorithmically."[11]

Let's consider theoretically how behavior can be gamed and manipulated online - how human judgment and decision making can be influenced and altered. Psychologist and Nobel laureate Daniel Kahneman proposed an innovative dual-process theory of human decision making; he described it as "Thinking, Fast and Slow[12]." Kahneman depicted two systems that the brain uses to process information, an automatic alongside a slower more deliberate mode of thinking. The two systems are active when we are awake and are constantly interacting. Kahneman explains System 1 as fast, intuitive and emotional, System 2 as slower, more deliberative and more logical:

> "System 1 runs automatically and System 2 is normally in a comfortable low-effort mode, in which only a fraction of its capacity is engaged. System 1 continuously generates suggestions for System 2: impressions, intuitions, intentions, and feelings. If endorsed by System 2, impressions and intuitions turn into beliefs, and impulses turn into voluntary actions[13]"

Now let's imagine an elaborate cyber behavioral persuasion, or indeed manipulation model, starting from a point whereby sophisticated cyber actors have harvested individual user data and created a comprehensive psychological profile. Operatives could then focus on a particular individual and manifest System 1 like impressions, metaphorically trapping the target in a series of filter bubbles, echo chambers and feedback loops, algorithmically reinforced by search and social technology content, normalized and socialized by network homophily, on the principle that 'similarity breeds connection.'[14] If endorsed by System 2, orchestrated impressions and feelings may turn into beliefs, and in effect over time could manifest as voluntary actions - such as voting.

To paraphrase Kahneman - manipulating, fast and slow.

Now let's consider such an operation at scale - a cyber-Machiavellian campaign, aided and abetted by machine intelligence. Undoubtedly there is a fine line between manipulative and persuasive technologies. For some, the use of the descriptor 'manipulation' may cause offense,

---

[11] https://www.wilsoncenter.org/blog-post/mass-killing-and-technology-the-hidden-links [12] Kahneman, D. (2011) *Thinking, Fast and Slow.* London*:* Penguin Group.

[13] Kahneman, D. (2011) *Thinking, Fast and Slow.* London*:* Penguin Group.

[14] https://www.annualreviews.org/doi/abs/10.1146/annurev.soc.27.1.415?journalCode=soc

with its connotation of victimology, devoid of personal agency and beliefs, whereas describing the same as 'persuasive' technologies is arguably more empowering for the 'human endpoint.' However, it is a moot point, as regardless of semantics, sentiment is being reinforced and impressions are being formed. Therefore, we should not dwell on the relative merits of arguing coercion versus persuasion. Instead, we need to focus on transparency.

Why? Because we have been here before.

The 'Oxford Handbook of Propaganda Studies'[15] details the infamous 'Subliminal Advertising Experiment,' describing how an offshoot of behavioral motivation research reared its ugly head in the 1950s:

> "45,699 movie patrons were "subjected to 'invisible advertising' that by-passed their conscious and assertedly struck deep into their subconscious." Once every five seconds, a message was flashed throughout a film for 1/3000th of a second—too fast to be seen by the human eye but supposedly long enough to be registered in the subconscious of the unsuspecting movie-goers. After "COCA-COLA" and "EAT POPCORN" were invisibly blinked on the screen, sales of each reportedly jumped (by 18 and 58 percent, respectively), these results quickly becoming the talk of not just Madison Avenue but also Main Street"

These advertisements targeted audiences at a subliminal level, at a sub-cognitive level "below thinking," that is, under human thresholds of sensation or awareness. In 1958 *Life* magazine noted that this form of 'subliminal persuasion' could be useful not just for selling products but for social initiatives such as anti-litter campaigns, and importantly in the context of this article, for promoting political candidates.

In an era characterized by the 'Red Scare,' the McCarthy hearings, and the Cold War between the Soviet Union and the United States the pervasive fear was that Madison Avenue "ad-men" could use mass propaganda to make people buy things they did not desire or need, or worse still, elect Soviet sympathizers into office.

And so, here we are in 2018. A few weeks ago, the Senate Select Committee on Intelligence completed its review regarding "Assessing Russian Activities and Intentions in Recent US Elections."[16] Reporting that "The leaders of the U.S. Senate Intelligence Committee… agreed with intelligence agencies' assessment that Moscow sought to interfere with the 2016 U.S. election to boost Donald Trump's prospects of becoming president[17]" House Republicans

---

[15] Auerback, J & Castronovo, R. (2013) *The Oxford Handbook of Propaganda Studies*. Oxford University Press: Oxford.

[16] https://www.burr.senate.gov/press/releases/senate-intel-completes-review-of-intelligence-community-assessment-on-russian-activities-in-the-2016-us-elections

[17] https://www.reuters.com/article/us-usa-trump-russia-committee/key-u-s-senators-no-doubt-russia-sought-to-interfere-in-u-s-election-idUSKCN1IH2AX

disagreed that Russia sought to boost the then Republican candidate Trump. Notably, Russia has denied interfering in the US election.

Earlier this year I had the opportunity to meet with Congressional staff to discuss the science of behavioral manipulation online. While I have the utmost respect and admiration for the dedicated and exhaustive nature of the investigation, I cannot help but observe that the parameters may have been somewhat restrictive, arguably limited by an explicit focus on Russian involvement. Perhaps a broader investigative remit may have had greater exploratory and therefore explanatory value. My concern is that many of the subtle nuances of the contemporary 'art of cyber war' may be lost in restrictive framing, for example:

- Creation of context in the cyber ecosystem;
- Environmental psychology of human behavior in cyberspace;
- Impact of subliminal algorithmic persuasive and manipulative technologies;
- Uncertain role of social technology enterprises – enablers, facilitators or bystanders;
- Continuously evolving strategic and networked global alliances;
- Ongoing development of capabilities particularly in artificial intelligence;
- Increasingly sophisticated technology-mediated interaction between candidates, campaigners, political consultancy services, data brokers, threat actors, hacktivists, nation-states and organized cybercriminals, the latter appropriately described by Europol as brokers of 'crime as a service' (CaaS) online[18].

Potentially, all of this, and so much more may be 'lost in investigation.'

Allegations of election interference are not confined to the US; the phenomenon is now global. 2016 was the year of the United Kingdom-European Union membership referendum, also known as "Brexit." A recent report by the US Senate foreign relations committee, titled "Putin's Asymmetric Assault on Democracy in Russia and Europe: Implications for US National Security" maintains that Russia attempted to influence the Brexit vote.[19] In May 2017, French voters were warned not to let fake news influence their vote in the then high-stakes presidential election following a 'massive hacking attack' on frontrunner Emmanuel Macron's campaign. The hacked documents, which were disseminated on social media by groups such as WikiLeaks, were dismissed by Macron's team as an attempt at "democratic destabilization, like that seen during the last presidential campaign in the United States."[20]

Interestingly there was reportedly little or no interference Russian or otherwise in the 2017 German elections. A key differentiator may have been that Germans primarily trust mainstream and traditional news media sources, and unlike the British, French, Americans and Mexicans they tend to be very wary of information disseminated on social technology platforms such as

[18] https://www.europol.europa.eu/iocta/2015/exec-summary.html

[19] https://www.theguardian.com/world/2018/jan/10/russian-influence-brexit-vote-detailed-us-senate-report [20] https://www.telegraph.co.uk/news/2017/05/06/watchdog-launches-investigation-massive-hacking-attack-emmanuel/

Facebook, WhatsApp, and Twitter. This seems to have made a difference. According to Sandro Gaycken, Director of the Berlin Digital Society Institute, which at the time was monitoring for Russian interference, they were "almost disappointed that nothing is happening…We don't see any verified attacks…We're not really expecting any Russian interference." [21]

The threat of Russian and Chinese interference loomed over Mexico's 2018 presidential election where over 3,400 elected positions at local, state and federal levels were at stake. However, evidence of external interference seems to be inconclusive, particularly regarding the use of bots, fake and automated social technology accounts. Ben Nimmo, a senior fellow at the Atlantic Council's Digital Forensics Research Lab stated that "There's no evidence to suggest that the political bots we found were based outside of Mexico," he highlighted that "Absence of proof does not equal proof of absence, but so far, there's no reason to suggest state-run efforts."[22]

The Mexican election witnessed a surge in web advertising and Internet campaigning; presidential candidates declared 159 million pesos ($7.8 million) were spent on online ads. Importantly, the election was characterized by allegations of foul play, foreign interference, and accusations of social-media coercion, bogus accounts, bots, paid influencers, trolls, online attacks and fake news. Reports suggest that Andres Manuel Lopez Obrador spent the least of the four presidential candidates on 'online propaganda.' In March of this year, according to the Mexico News Daily analysts estimated that bots or influencers were creating some 18% of Mexican Twitter content [23] However, it seems that rather than utilizing bots or paid influencers, Obrador's team set about organizing a network of some 400,000 volunteers, described as 'amplifiers,' and tasked them with disseminating campaign content.[24] On Sunday the 1st of July Lopez Obrador was elected President of Mexico in a landslide victory, it would appear that a human-centered approach and attempting to 'play fair' in Cyberspace resulted in real-world electoral success.

It is useful to consider the relationship between online political campaigning and significant national threats. Governments are becoming increasingly aware of the prevalence of PsyOps (psychological operations) or in the digital sphere, 'CyberPsy Ops.' That is, what can only be described as socially engineered attacks on a national scale attempting to manipulate mass populations into acting – attempting to interfere with democratic process whether it's the US Election, the UK, France, Germany or the recent Mexican election. As Professor Sir David Omand[25] has noted "just as criminals can exploit cyberspace to conduct both cyber-assisted and cyber-enabled crime, so nation states and non-state groups can use the capabilities of the Internet both to disseminate their narratives and world-views directly and to exploit the unique

---

[21] https://www.nytimes.com/2017/09/21/world/europe/german-election-russia.html

[22] http://www.businessinsider.com/russian-bots-are-accused-of-meddling-in-mexicos-election-2018-6

[23] https://mexiconewsdaily.com/news/trolls-bots-fake-news-are-campaign-tools/

[24] https://www.reuters.com/article/us-mexico-election-spending/mexico-presidential-campaigns-ramp-up-spend-on-online-ads-idUSKBN1JI01X

[25] Omand, D. (2018) The threats from modern digital subversion and sedition: Journal of Cyber Policy https://www.tandfonline.com/doi/abs/10.1080/23738871.2018.1448097

characteristics of the digital space to coordinate and mount covert influence operations and 'active measures'"

In terms of behavioral manipulation online *subversion* can be defined as external interference in a nation's affairs, arguably being carried out by foreign state and threat actors who are gaming processes remotely. *Sedition* can be conceptualized as internal dissent manifesting in the form of a coerced and often misinformed public that may ultimately be considered as an insider threat on an unprecedented national scale.

It costs a lot of money and resources to become a superpower in the physical-world – in Cyberspace, all it takes is a handful of brilliant computer scientists and a lot of computing power. However, let's not forget that "it's complicated" on the cyber frontier. The elephants in the cyber room – China and Russia – are consistently named and shamed in an exercise that often resonates with 'round up the usual suspects.' While weaker state actors jockey for position, trying to become stronger and seeking power status, non-state actors pursue their idealistic goals, and technology enterprises operate under the radar with little thought given to their potential aspirations of statehood.

The military successfully navigates threat landscapes informed by situational awareness - the challenge for many countries is to develop situational awareness in Cyberspace, or increasingly face situations where intent is obfuscated, attribution is difficult and hybrid threats progressively undermine national security. [26]

There are very few people worldwide who are experts in cyberpsychological operations, most of them probably work in international cyber war labs, or in private enterprise – some of us are ethical 'white hats' operating in this space. There is a lack of focus on, and a paucity of solutions to evolving hybrid threats, therefore we need to "*get rid of all the illusions"*[27] and recognize the nature and scale of the problem; we need to understand the inherent cyber vulnerability of our societies in physical and human terms; we need to invest in training and upskilling of detection, intervention, and defense personnel; and we need to develop sophisticated machine intelligence solutions that can cope with the volume, variety, velocity and veracity of these threats to national security, and to democracy.

The Internet has been conceptualized as an 'infrastructure'– similar to a motorway or a railroad – the Net may be many things, but it is not merely an infrastructure. The unprecedented connectedness offered by the Internet means that it has an inescapable and profound effect on humankind - on the individual, and on the group. Therefore, there is an urgent need for a new scientific approach, regarding research, analysis and insights concerning human behavior mediated by technology. When it comes to the Internet, and particularly problematic behaviors

---

[26] "any adversary that simultaneously and adaptively employs a tailored mix of conventional, irregular, terrorism and criminal means or activities in the operational battle space"

[27] https://www.memri.org/reports/st-petersburg-international-economic-forum-plenary-meeting

online – we need academic first responders[28]. We need experts who can illuminate that intersection between humans and technology. The task for cyberpsychology is to continue to build up a body of literature on how humans experience cyberspace, the scope for research is infinite, from the gaming of the homophily principle, to how filter bubbles may be destroying democracy. The scope for insight is immeasurable.

The critical task in forensic cyberpsychology is to scientifically focus on how threat actors, nation-state or otherwise, undertake secret influence operations and conduct active measures in cyber environments. To date efforts have concentrated on finding technological solutions, arguably without due consideration of how human behavior develops, presents, mutates, amplifies and accelerates in cyber domains or understanding of the interdependent relationship between Cyberspace and the real-world, and without in-depth examination of how machine intelligence may affect human behavior in this ecosystem.

"Locards Exchange Principle"[29] dictates that every contact leaves a trace – this is also true online, however, as discussed, verification and attribution are problematic. We understand the premise of real-world staging of a crime scene, the planting or manipulation of physical evidence – for example, a bloodied glove placed at a crime scene. However, little thought is given to the potential to stage a cybercrime scene – a phenomenon I describe as *cyber staging*[30]. Focusing all our investigative efforts on Russian interference in the US, or even the recent Mexican election may be restrictive and myopic, particularly when evidence can be cyber-staged. Of course, paid advertisements placed by the Internet Research Agency (IRA) a notorious Russian "troll" farm[31] could be a trail of evidence, or equally they could be a digital red herring, an exemplification of a former superpower leveraging an opportunity in Cyberspace to write themselves into the narrative – to put Russia into play.

At this point, I worry less about who did it, and more about the fact that it can happen – my focus is on human vulnerability mediated by the Internet, the Achilles heel of a voting process. Solutions lie in an ethical approach, in transparency; in tackling the scourge of misinformation and disinformation, but mostly answers lie in addressing one of the 'sacred cows' of the Internet - anonymity. Let's imagine a Cyberspace where fake news and phony social media accounts are eradicated, a space free of anonymous trolls and malicious bots, a domain liberated from operatives conducting covert active measures.

We need to debate the introduction of *nonymous*[32] protocols in the environment of Cyberspace to counter the often-toxic effects of anonymity – the superhuman cloak of invisibility that comes with great power, but is consistently abused online. We need to discuss this, for

---

28 http://www.maryaiken.com/cyber-effect/
29 https://www.forensichandbook.com/locards-exchange-principle/ 30 https://www.lawlibrary.ie/News/TheBarReview_April2018_web.aspx 31 https://democrats-intelligence.house.gov/social-media-content/
32 https://neologisms.rice.edu/index.php?a=term&d=1&t=9877

ourselves, for our societies, for our new frontier, and for the greater good, but most of all for the preservation of democratic process.

Let's not forget that freedom of speech, is dependent on freedom of thought – do we want to allow opportunistic forms of systematic subliminal cyber manipulation, fast and slow to thrive? These 'dark tools' provide a modus operandi for those who seek to polarize opinion, and disrupt the status quo, motives range from individuals with a hacktivism belief system to what Madeline Albright has described as the rise of fascism[33]. To sustain free and fair elections we must demand transparency in the new environment of Cyberspace.

My forensic observation is that when an analyst finds a Russian bot, a paid advertisement, or traffic purportedly from China the question of cyber staging must be considered. Ultimately interference in elections whether in Europe, North or South America cannot merely focus on 'Reds under the Algorithm.' In an ever-increasing mountain of big data, it would appear we cannot see the forest for the trees – but then sometimes it's not that complicated.

The answers and solutions are there, logical and apparent.

Hidden in plain sight.

Dr Mary Aiken, Cyberpsychologist and Author of 'The Cyber Effect'
Global Fellow, Digital Futures Project, The Wilson Center.
Adjunct Associate Professor, Geary Institute for Public Policy, University College Dublin.
Academic Advisor to the European Cyber Crime Centre (EC3) at Europol

33 https://www.washingtonpost.com/outlook/is-the-united-states-really-on-the-road-to-fascism/2018/04/13/9e66d45a-3e26-11e8-8d53-eba0ed2371cc_story.html?noredirect=on&utm_term=.3fc983205154