Truth Dies First: Storyweapons on the InfoOps Battlefield

Renny Gleeson

Storyweapons are adversarial narratives that use algorithms, automation, codespaces, and data to hijack decision-making, and the stories of who we are, what we believe and why it matters. They leverage vulnerabilities and weaknesses against people and populations; they subvert freewill to bend actions to self-sabotage. Storyweapons exploit attack vectors across our new mixed reality of code and cognition, and they move the frontlines into the minds and software connected to any strategic objective. Defending the US against storyweapons requires a reconsideration of battlefields, operational models, and threat actors.

Storyweapons are a new class of threat, fielded by new threat actors in non-traditional domains across the new landscape of Codespace. A military "prepared to fight the last war" risks missing the one raging now: storyweapons are evolving, mutating, and redefining how we wage war and peace in real-time. To "defend the United States against all enemies" means defeating foreign and domestic adversaries who use storyweapons to attack our democracy, our institutions, and our people. They are doing it right here, right now, and from every screen, weaponizing the information environments and the connected spaces in which we live. "The future of disinformation is domestic," noted Alex Stamos, Facebook's former security chief [1].

To unpack storyweapons, we first must know why the "story" is important.

Maybe you know the story about the astronaut's pen. It goes something like this: Back in the sixties, American astronauts needed something to write with in space, so NASA put in years of research and spent millions of tax dollars to develop a pen that could work up there. A masterpiece of engineering, it had pressurized ink and a carbide-ball tip so it could write upside down and in zero G. The Soviets, well they had the same problem. They gave their cosmonauts pencils. It's a great story, but it's not true.

© 2020 Renny Gleeson

Renny Gleeson works at Wieden+Kennedy (W+K), the world's largest independent creative ad agency. W+K handles some of the world's most well-known brands, and was named "Agency of the Year" the last three consecutive years. Renny joined W+K in 2007 to lead interactive strategy, and served on the global management team. In addition to direct client work, he co-founded and led W+K's tech/business accelerator and now leads W+K BIG, the W+K Business and Innovation Group focused on business and brand experience transformation. An industry leader and TED speaker, he writes, studies, and speaks on persuasive technologies and the ways they shape and are shaped by human behavior. The views expressed here are his own.

Truth seldom matters when it comes to stories - what matters is how they feel. Just look at our political situation. The truth about the pen is that a private company developed the pen at its own expense. As for pencils, they introduce flammable material into the cabin and can generate broken lead, a threat to astronauts and their equipment. The truth is that once the pen was invented, the Soviets ordered them from the same company.[2] But "truth alone," as Carl von Clausewitz wrote, "is but a weak motive of action with men...the strongest impulse to action [is] through...feelings"[3]: the 'astronaut pen' is a story that feels *true enough* - it resonates, and stories that resonate, propagate. Along the way, our most deeply felt stories become foundational to our individual and collective identity. At that level, they become impervious to truth. We pay no attention to facts that put those stories at risk; from a sensory standpoint, we literally do not see them. As Daniel Kahneman wrote in Thinking Fast and Slow, "The confidence that individuals have in their beliefs depends mostly on the quality of the story they can tell about what they see, even if they see little."[4] Stories—especially the deep stories that exist beyond words and rationality—do not describe reality; they are the filters through which we create it.

Our stories are more vulnerable than we know: our cognitive systems are hackable by everyone, from kids' birthday party magicians to infowar adversaries. We do not see the flaws in those systems because they are features of the systems. Storyweapons leverage the infrastructure of perception to misguide, misdirect, and manipulate.

We interpolate "meaning" not from f*acts* but from estimations of relationships between them. Interpolation enables us to build stories from intuitive leaps, using extremely limited data, but the trajectory of those leaps (and where we land) is influenced by our biases, heuristics, hacks, and filters operating below

conscious cognition. Sensory information is filtered first through the amygdala (our "reptile-brain" of "fight-or-flight") then through the mid-brain limbic system (our emotional/feeling brain) before reaching the frontal lobe (our rational/thinking brain). By biological design, outrage, fear, and the unfair light up these lower regions, grab the spotlight of our attention and short-circuit rational thought. This functional truth renders us vulnerable to adversarial attacks through media and software-mediated platforms. It also makes us vulnerable to attention hijacking by the platforms themselves, who monetize our attention in service to advertisers and third parties. They compete to grow attention share and revenue, and that competition becomes a race down the brain stem: research shows that joy moves fast over social networks, "but nothing is speedier than rage."[5] The ruthless economic imperative behind the zero-sum wars for attention has fueled the rise of outrage as a business model in the places we connect with who and what we love.

Knowing what makes and motivates someone provides an instruction manual for actuation. A study by Gloria Mark at UC Irvine[6] showed one could predict the "big five personality traits" —Openness, Conscientiousness, Agreeableness, Extraversion, and Neuroticism—to 80% accuracy based on click streams, interactions, and behavior. This is precisely the data Cambridge Analytica leveraged to achieve their clients' goals. What we *do* online is who we are, and we are online all the time: our digital signatures and data contrails lay bare our deep stories and our subconscious biases, filters, and desires. Adversarial Artificial Intelligence and Machine Learning systems that access our behavioral data can weaponize things about us we do not even know ourselves. Those adversaries are full-spectrum—one major US insurance company used its algorithms to predict how high insurance rates could be jacked up before a customer would switch to another provider; a 2019 U.N. report[7] suggested that with the advent of facial recognition software, eye-tracking and dynamic voice sentiment analysis, we might need to legally protect the right to dishonesty. When we touch software, or software touches us, we are known.

Software no longer sits safely behind the glass of our computer monitors or mobile devices; it permeates our environments, introduces new functionalities and vulnerabilities, and transforms decision-making, and the frameworks within which decision-making takes place to create new, symbiotic *decision spaces*.

Software, like gravity, has become a fundamental force of human experience—it can't be talked about in a discrete domain, because it affects all domains. Our stories move through, shape, and are shaped by software; it has fused the physical (what you see), informational (what you capture/organize), and cognitive (sense-making, or CogSpace) domains to create the new world—and battlefield—of *Codespace*.

The interplay between CogSpace and CodeSpace is a continuum of heavily contested Information Environments. CodeSpace's algorithmic "decisions" determine and reframe the

raw materials we use to sense-make in CogSpace; CogSpace's narrative-influenced human "decisions" generate data that inform CodeSpace "learning," dynamic reconfiguration and outcome-based optimization.

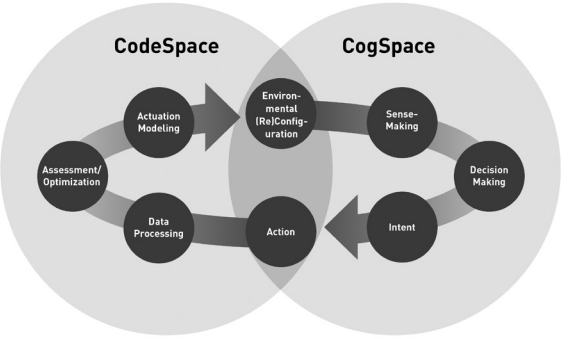

Figure 1: Storyweapon Threat Landscape

In these new decision spaces, we make conscious and unconscious decisions based on software, with software making decisions based on us. Our environment itself is alive, learning, aware. It has memory, biases, and opinions. Actors—private and state, foreign and domestic—fight for their agendas and our attention in these spaces; their actions and algorithms generate the raw materials of sense-making we use to build our stories of truth, identity and meaning.

Codespace was coined in 2014 by Kitchener and Dodge to describe what they called "life-as-software-mediated-experience"[8]. A typical airport demonstrates their premise: software is used to book your flight, integrate that flight into your calendar software, call a car to the airport, check you in, process and route your luggage; navigate you through security, determine your identity/threat level/processing path; tell you your gate, access public Wi-Fi or private "hotspots," keep you entertained while you wait, dynamically alert you to departure and arrival time changes, enable plane access and status perks, and then fly the plane to your destination. An airport without code isn't an airport—it's a shed full of angry people surrounded by metal paperweights full of jet fuel. Airports are Codespaces.

Codespaces blur the lines between software, hardware, and experience; they will evolve to deliver customized video, audio, and haptic experiences. Google search results are already different for each user (based on historical searches and online behavior); soon real-world experiences will be, too: in the fall of 2020, some Detroit Metropolitan Airport travelers will experience custom visual beamformed airport signage (ala Minority Report) linked to their boarding pass, preferences, and physical position. Two travelers, looking at the same sign, will see different messages. "Dark marketing," made notorious by the Cambridge Analytica revelations, is digitally targeted micro-persuasion, impossible to see as a whole, invisible to all but the targeted mind, vanishing once the emotional payload is delivered to the brainstem. Codespace enables this in the real world.

We will be alone together: two people looking at the same thing at the same time will sense different things. When lived experience is addressable, it becomes relative and vulnerable—and everything will be addressable. IPv6, the new Internet protocol being globally rolled out, has created enough new addresses to uniquely connect every atom on this earth to the Internet, with enough left over to connect 100+ more earths[9]. In self-optimizing addressable codespace, the truth becomes relative.

Storyweapons exploit all these technologies and more: the doctored video that tells us stories that reinforce our "illusory superiority"[10] will become augmented realities that amplify polarization; "beam-forming" will deliver micro-targeted visual, auditory, and haptic experiences in the real world, undetectable to anyone but the intended recipient; synthetic entities will be able to call, text or video chat with you, dynamically evolving their responses to your voice signature or facial expressions. Storyweapons will use a continually evolving tactical toolkit against people on the physical battlefield and use codespace to bring everything connected to combatants into the fight as well. War will not be fought "over there," it will be fought in your mind, your home, your social connections, and in the court of public opinion.

Codespaces are battlefields that will dynamically reconfigure decision spaces and rewrite perception. By 2025, it is estimated that 5G will achieve 15% penetration globally and 74% in the US[11]; a functional promise of 5G is sub-1ms *latency*, the time it takes for your input through a software interface to generate an outcome. High latency is why the maps app on your phone tells you to take an exit after you've passed it on the freeway; low latency might win you the battle royale in Call of Duty's Warzone. Biologically, neural processing is such that our perception of reality lags actual reality by about a tenth of a second[12]. Codespace operating with sub-1ms latency is a reality that can change in response to our feeling brain before our thinking brain consciously experiences it.

Three reasonable assumptions about Codespace operations include:

1. ***Everything is compromised.*** Every interaction with Codespace generates, shares, and potentially leaks behavioral data. Hardware and chipset suppliers answer to their nations of origin (e.g., China's National Intelligence Law). Social software experiences are powered by supercomputer arrays running algorithms that exploit our weaknesses and vulnerabilities to serve third-party agendas, learning, and self-optimizing at the speed of light. Finally, codespace is networked "systems of systems" with all the interoperability, incompatibility, integration and software updates and security patch headaches that implies. The Codespace we live in is neither safe, nor housetrained. Any software-mediated experience or enabling connection is an attack vector for storyweapons.
2. ***Vulnerability is a feature, not a bug.*** More connections = more sensors = more data = more value. Connecting all those things—your printer, your coffeemaker, your thermostat—has to be easy or we would not buy them. According to security researchers

in 2017, having just five passwords would have allowed access to 10% of the world's estimated 8.4B Internet-connected objects whose users had not changed their original password[13].

3. ***Attack vectors multiply exponentially, not linearly.*** Codespace environments are seldom single-author systems. Expect Frankenstein-ed systems of systems: a shit-sandwich of cascading dependencies and budget-restricted kluges running new and legacy hardware, multiple software configurations, and generations-old, unpatched security. These systems can be their own worst enemies even before adversaries compromise them.

Everyone and everything that touches software is effectively on the new Storyweapon battlefield; there is no "behind the lines." All an adversary needs to secure "narrative" or "reflexive" control is enough data to tell the story you want to hear. And that story doesn't have to be true, it only must to be *true enough*.

The most effective marketing does not sell you a product; it sells you the story that the product tells about you, an emotional and aspirational story of who you'd be with that product in your life. We vote for the best stories with our attention. And if that story is compelling enough, if it feels true enough, it might break through the wall of 5-10,000 brand messages[14] and 12.5 hours of media we consume daily[15]. If we see in it something we want to believe about ourselves, we might splice elements of that story into our *deep story* DNA. Done at scale, you can sell product, move markets, shape opinion, and drive action.

You can't beat a "true enough" storyweapon with facts.

The only way you beat a story is with a better one.

To field a storyweapon tailored to its target, one needs data. One can steal data to build targeting profiles—38 Billion customer data files have been breached or hacked in the US alone since 2010[16]. You also can do what marketers do: buy it from the AdTech players fighting it out in the $7 Trillion dollar attention industry. ChiefMartech's annual roundup lists 7,040+ marketing tech companies (up from 150 in 2011)[17] —for illustration purposes, consider just three: one is a data aggregator that claims to have dynamic, ongoing location data for 25% of the world's population; a second provides a mobile application that aggregates the data from 100 Billion data transactions by 1.4 Billion people across more than 7 Billion devices. At the CyCon U.S. conference in Washington DC in November of 2019, speaker Admiral (Ret.) Mike Rogers told attendees that China's government had amassed "2,500 data points per citizen"; four years prior, our third example, a US data brokerage subsequently acquired by an ad agency holding company bragged it had over 5000 data points per person[18]. When a single company on a roster of over 7,000 can make China's state surveillance look amateur, you must wonder about the rest. The sheer volume of legally and illegally available data makes it conceivably possible for any actor, foreign or domestic, to have already developed profiles for every potential "target of interest," including everyone and everything connected to them.

Silicon Valley venture capitalist Marc Andreessen has said, "software is eating the world,"[19] - our new reality is what's coming out the other end: convenience and connection, and also relentless wars for narrative control, storyweapons of micro-targeted persuasion and behavior modification at scale, and Codespaces of predictive actuation.

Fighting these wars across mental, physical, and Codespace geographies will require new operational models. For example, the ad agency where I work bases organizational structure on slime mold, a networked organism that coalesces from slime into a collective, mobile being, purpose-built to achieve specific goals, which, once achieved, returns to its original state. As the landscape of persuasive communication has evolved, this structure has allowed maximum flexibility and resilience. Another active-defense model is the human immune system, and how it identifies and assesses potential threats, and distinguishes them from healthy tissue.

To "defend the United States against all enemies" means we must effectively counter attacks on our democracy, our institutions, and our people from without or within. We cannot allow the American experiment to "die by suicide" under our watch. General (Ret.) James Mattis noted, "a proper understanding of our national story is absent"[20]. In that void we have allowed attack vectors on our societal cohesion to be built around us, enabled by direct access to the minds of American citizens. To counter effectively, our forces must be opportunistic, flexible, and adaptable, able to 'defend forward' at home and abroad against enemies domestic and foreign—with a force that is a hybrid of public, private, and military actors, flexible, resilient, and purposeful-built to defend our stories, and to win on the Storyweapon battlefield.

Stories will make or break us. We need storywarriors on the field, fighting for the best version of America. The American story will be pivotal in the decade-to-come as our decisions determine whether Codespace becomes a prison of insular micro-realities, or a launch pad for a greater good. The health and continued viability of the American experiment hinges on the result. We face a nation-wide collapse of journalism (the critical watchdog of a democratic society), accelerating climate disaster, and widening income and opportunity inequality. We will be living with the impact of COVID-19 for years to come, and already, the mis- and disinformation campaigns are ramping up for the 2020 presidential election cycle. Now more than ever, we cannot allow our stories to be written by our adversaries.

This is our chance to take the fight to those who would train Storyweapons on our people—and make others think twice about ever doing it again. We do not always get to choose when we fight, but we do get to choose what we fight for.

What new stories will we write?

NOTES

1. Sheera Frenkel, Nicole Perlroth, and Kevin Roose, "Tech Giants Prepared for 2016-Style Meddling. But the Threat Has Changed", *The New York Times*, March 29, 2020, https://www.nytimes.com/2020/03/29/technology/facebook-google-twitter-november-election.html.
2. Ciara Curtin, "Fact or Fiction?: NASA Spent Millions to Develop a Pen that Would Write in Space, whereas the Societ Cosmonauts Used a Pencil", *Scientific American*, December, 2006, https://www.scientificamerican.com/article/fact-or-fiction-nasa-spen/.
3. Carl von Clausewitz, On War, (Penguin Classics,1982), 159.
4. Daniel Kahneman, Thinking, Fast and Slow, (FSG Adult; 1st ed., 2013).
5. Matthew Shaer, "What Emotion Goes Viral the Fastest", Smithsonian Magazine, April, 2014, https://www.smithsonianmag.com/science-nature/what-emotion-goes-viral-fastest-180950182/.
6. Noah Ganzach and Gloria Mark, "Personality and Internet usage: A large-scale representative study of young adults", *Computers in Human Behavior*, V.36 2014/07/01, 274–281, https://www.researchgate.net/publication/262016396_Personality_and_Internet_usage_A_large-scale_representative_study_of_young_adults.
7. Clement Bellet and Paul Frijters, "Chapter 6: Big Data and Well Being", *World Happiness Report,* (Sustainable Development Solutions Network - March 2019) sec 3.2, "Privacy and Conclusions," https://worldhappiness.report/ed/2019/ https://worldhappiness.report/ed/2019/.
8. Martin Dodge and Rob Kitchin, Code/Space: Software and Everyday Life, (Boston: MIT Press, 2014).
9. Steve Leibson, "IPV6: How Many IP Addresses Can Dance on the Head of a Pin?", *EDN.com,* March 3, 2008, https://www.edn.com/ipv6-how-many-ip-addresses-can-dance-on-the-head-of-a-pin/.
10. "Illusory Superiority" is a cognitive bias referenced in the "Dunning-Kruger effect", *Wikipedia.org,* https://en.wikipedia.org/wiki/Dunning%E2%80%93Kruger_effect.
11. Global figure from "New GSMA Study: 5G to Account for 15% of Global Mobile Industry by 2025 as 5G Network Launches Accelerate", *GSMA.com*, February 25, 2019, https://www.gsma.com/newsroom/press-release/new-gsma-study-5g-to-account-for-15-of-global-mobile-industry-by-2025/; US figure from "Ericsson Mobility Report", Ericcson.com, November 2019, accessed: https://www.ericsson.com/4acd7e/assets/local/mobility-report/documents/2019/emr-november-2019.pdf.
12. George Musser, "Time on the Brain: How You Are Always Living In the Past, and Other Quirks of Perception", *Scientific American Blog*, September 15, 2011, https://blogs.scientificamerican.com/observations/time-on-the-brain-how-you-are-always-living-in-the-past-and-other-quirks-of-perception/.
13. Josh Fruhlinger, "The Mirai Botnet explained: how teen scammers and CCTV cameras almost brought down the internet", CSOonline.com, March 9, 2018, https://www.csoonline.com/article/3258748/the-mirai-botnet-explained-how-teen-scammers-and-cctv-cameras-almost-brought-down-the-internet.html.
14. Jon Simpson, "Finding Brand Success in the digital world", Forbes.com, August 25, 2017, https://www.forbes.com/sites/forbesagencycouncil/2017/08/25/finding-brand-success-in-the-digital-world/#7d22a42e626e.
15. "Average Time Spent per Day with Total Media (2017-2021), eMarketer, November 2019.
16. Megan Leonhardt, "The 10 Biggest Hacks data hacks of the decade", CNBC.com, December 27, 2019 - https://www.cnbc.com/2019/12/23/the-10-biggest-data-hacks-of-the-decade.html.
17. Scott Brinker, "Marketing Technology Landscape Supergraphic (2019): Martech 5000 (actually 7,040)", accessed March 15, 2020, https://chiefmartec.com/2019/04/marketing-technology-landscape-supergraphic-2019/.
18. Jeff Chester, "Acxiom: "For every consumer we have more than 5,000 attributes of customer data", Center for Digital Democracy, January 10, 2014, https://www.democraticmedia.org/acxiom-every-consumer-we-have-more-5000-attributes-customer-data.
19. Marc Andreessen, "Why Software Is Eating The World", *The Wall Street Journal*, August 20, 2011, https://www.wsj.com/articles/SB10001424053111903480904576512250915629460.
20. James Mattis, "The Enemy Within," *The Atlantic*, December 2019, 102. 20. James Mattis, "The Enemy Within," *The Atlantic*, December 2019, 102.