ARMY CYBER INSTITUTE AT WEST POINT PRESENTS

INVISIBLE FORCE

INFORMATION WARFARE AND THE FUTURE OF CONFLICT

INTRODUCTION BY

P. W. SINGER & AUGUST COLE

AUTHORS OF *GHOST FLEET: A NOVEL OF THE NEXT WORLD WAR*

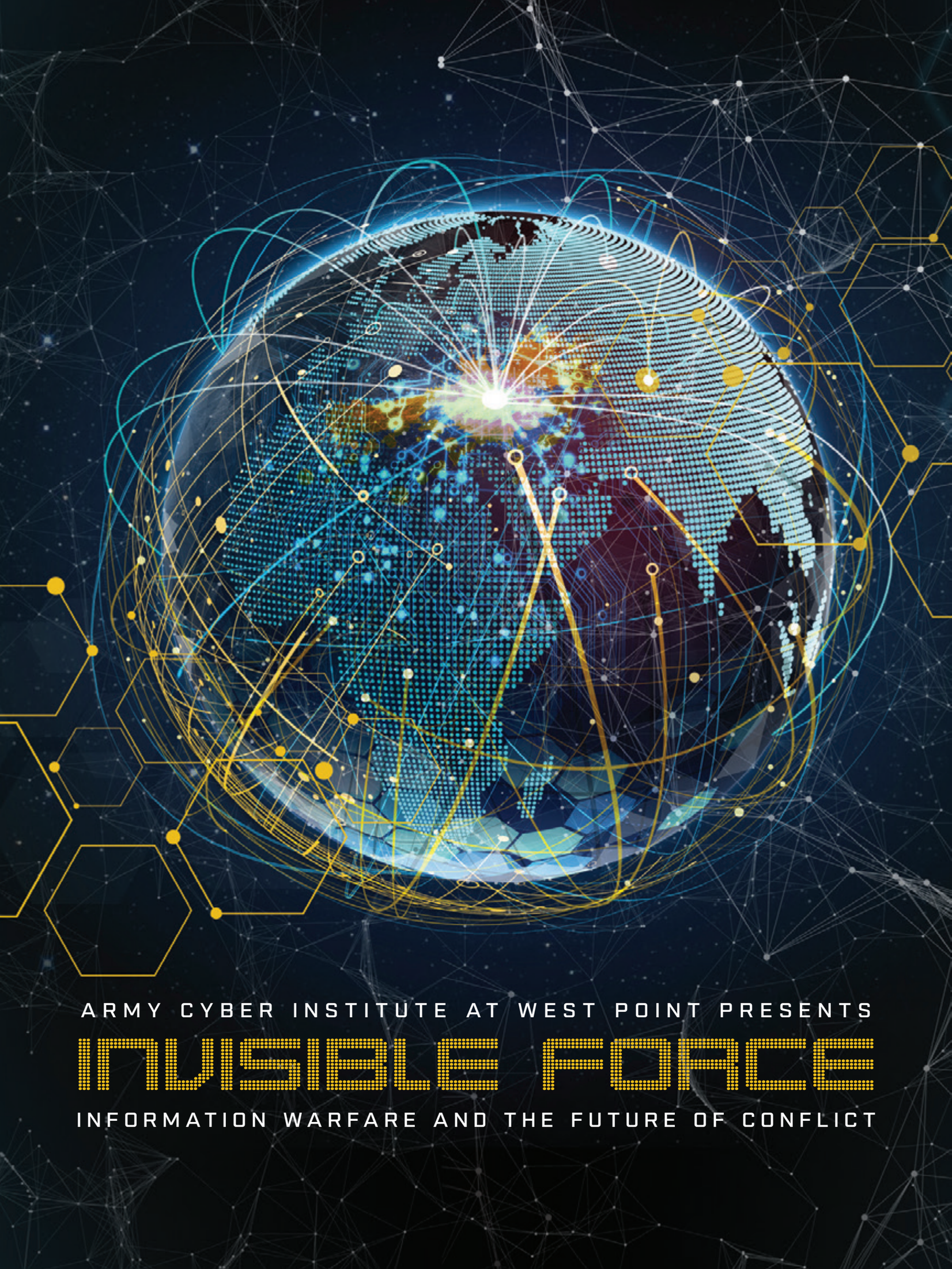
The global adoption of powerful network technologies is creating effects on human cognition which are continuing to challenge, if not erode entirely, the ways in which democratic societies govern and defend their people. In an increasingly connected world, individuals now have the power to instantaneously broadcast images and perspectives of world events in a manner that has traditionally been reserved for trusted media sources. The erosion of the gatekeeper's authority has enabled diverse perspectives to flourish, but also comes with a cost. This fact has created a situation in which the value of information is based on its ability to go viral as opposed to its truth and accuracy. Modern technology has created a world in which information scarcity is being replaced by information overload. It is a world where narratives are being created to manipulate human emotion, bias, and the social construction of truth in ways that are creating a post–truth era. How does the military engage in an era where information can be both true and false simultaneously, dependent upon the audience's perspective?

As more of the world's population embraces these powerful technologies, the more our adversaries adopt nefarious methods to exploit these vulnerabilities in the homeland and within our area of operations abroad. Adversaries of our great democratic nation can now simultaneously shape the narrative domestically and internationally during strategically important military operations. Nowhere have the effects of networked technologies been more demonstrated, time and again, than in the conflicts that have occurred thus far in the 21st century. Globally connected information technologies enable our strategic competitors to achieve their aims and objectives in domains that are short of armed conflict.

The intent of this graphic novel is to influence the thinking of U.S. leaders developing future policies, processes, and systems that will enable us to disrupt, mitigate, recover, and defeat any nefarious uses of technology by competitors and adversaries alike, in future information–age conflicts. The U.S. military exists in an era of great transition. We are pivoting from missions focused on combating terrorism and reorganizing to conduct large–scale combat operations in an era of great power competition. Currently, we find ourselves applying industrial–age organizations, strategies, and even technologies to information–age problem sets. We need new tools to help the Army develop novel frameworks of thinking about the fight we will face in the future. As a result, the Army Cyber Institute's information warfare team, in collaboration with Arizona State University, spent a year applying strategic foresight methodologies that developed the science fiction prototypes illustrated in this graphic novel. The Army Cyber Institute at West Point's mission is to influence the U.S. Army's vision for the future and to develop military leaders of character that will confront these futures.

– Lieutenant Colonel Robert Ross, Ph.D.
Chief Research Scientist
Information Warfare Team Lead
Army Cyber Institute

Disclaimer: The views expressed in this book are those of the authors and do not reflect the official position of the U.S. Government, the Department of Defense, the Department of the Army, or the United States Military Academy. This book is a work of fiction. Names, characters, places, and incidents are the product of the author's imagination or are used fictitiously. Any resemblance to actual events, locales, or persons, living or dead, is coincidental.



ARMY CYBER INSTITUTE AT WEST POINT PRESENTS

INVISIBLE FORCE

INFORMATION WARFARE AND THE FUTURE OF CONFLICT

Science Fiction Prototypes are science fiction stories based on future trends, technologies, economics, and cultural change. The story you are about to read is based on threatcasting research from the Army Cyber Institute at West Point and Arizona State University's Threatcasting Lab. The story does not shy away from a dystopian vision of tomorrow. Exploring these threats inspires us to build a better, stronger, and more secure future for our Armed Forces.

CONTENTS

INTRODUCTION:

PUSHING THE CREATIVE ENVELOPE FOR AN OPERATIONAL EDGE

PETER W. SINGER AND AUGUST COLE, AUTHORS OF *GHOST FLEET: A NOVEL OF THE NEXT WORLD WAR*

Drones fill the sky over a shattered city.

Refugees navigate their way through a violent conflict zone.

Gowned and masked doctors combat a fast-moving viral outbreak.

From the first panels of *Invisible Force*, it's clear that this is no ordinary comic. But this graphic novel is a glimpse not only into the future of war — but of the future of professional military education: engaging, visceral, and easily accessible. To be sure, the study of Clausewitz and the Battle of Bull Run aren't going anywhere. But we are at a moment of incredible change, not just in the world around us, but in the tools we use to understand it. New forms of communication and education, including the comics considered by many as only for entertainment, are emerging as a critical tool among U.S. and allied militaries for exploring what the future operating environment really holds.

The Army Cyber Institute at West Point is among the leaders of this movement with its series of graphic novels. This is no easy thing, not just in taking the plunge into such an unorthodox approach, but executing the work required to pull it off. The number of collaborators needed to produce a compelling graphic novel, also called a Science Fiction Prototype, can easily run into the dozens, ranging from writers and subject matter experts to illustrators and colorists. Yet it is the harnessing of such diverse skills that produces can't-put-this-down storytelling and conveys the organized creativity that is also needed to win in the operating environment. As an example of collaborative innovation, there is none better, for the very reason that there is nowhere to hide in a graphic novel. The prior volume, *Dark Hammer*, demonstrated that an exquisitely executed graphic novel with myriad characters can provide an unflinching look at tomorrow's high-intensity wars, particularly as the American military grapples with its dependence on technology. *Invisible Force* continues with a nuanced tale of vulnerability, and the way that individual soldiers will need to be able to think, act, and operate in unconventional ways to accomplish missions that seem insurmountable if approached in a conventional manner. But it does so in a manner that dazzles the eye, while pulling at emotions.

Breaking with convention is at the core of the larger "FICINT" concept — the fusion of fictional narratives and intelligence — that is another tool to use alongside signals or human intelligence sources. FICINT is not about pure creativity, however. It is the method of creating and curating "useful fiction" grounded in real-world research that would be familiar to a political scientist or technologist. The growing acceptance of this approach is a recent phenomenon that runs alongside the march of innovation around the world in technologies that range from the purely military, such as hypersonic missiles,

> ***INVISIBLE FORCE* IS ULTIMATELY A STORY ABOUT THE POWER OF IDEAS AND THEIR SIMULTANEOUS STRATEGIC INFLUENCE ON BOTH SMALL GROUPS OF PEOPLE ON UP TO ENTIRE POPULATIONS.**

to ones that began as civilian, like AI-driven social media algorithms, but now have immense military relevance. The old foresight and analytical methodologies are insufficient to fully capture or forecast the democratization of technology, but also struggle to identify the emergence of new actors and adversaries whose methods and objectives look nothing like past foes.

This FICINT approach is catching on around the world, literally, as a form of professional military education (PME) that is as much about mind-opening thought experiments as revealing hidden truths that current doctrine and assumptions might gloss over. Every single U.S. military service has joined in. At West Point, the Modern War Institute has published fiction and has bestselling science fiction and graphic novel writers like Max Brooks as fellows. The U.S. Naval Institute's storied *Proceedings* magazine may date back to 1874, but it now publishes futuristic science fiction and graphic novels that are now well established in the Institute's catalog. So, too, did the Marine Corps Warfighting Lab turn to science fiction stories and graphic novel illustrations to showcase their more traditional futures forecast, and ended up having more Marine readers than any of their official strategy documents, illustrating another value of FICINT — a wider reach. From a ground-up innovation point of view, the crowdsourced *Destination Unknown* graphic novels produced by a team of creatives and Marines affiliated with the Marine Corps University Brute Krulak Center for Innovation and Creativity attest to a groundswell of narrative innovation. At the Air Force's Air University, its elite Blue Horizons fellows now get schooled up on science fiction narratives each year, including how to read graphic novels for professional development. Allies such as Australia prominently feature science fiction at their main defense college, both in terms of reading and conferences. "Reading science fiction provides variety in honing the intellect of a military officer," writes General Mick Ryan, commander of the Australian Defence College, who also edited a project of real-world lessons on military strategy derived from *Star Wars*. While in Europe, NATO Allied Command Transformation and the British and Norwegian armies have also used FICINT stories and illustrations to place readers right in the middle of the technologically complex and politically chaotic conflicts of the 2030s and 2040s.

When weighing the 21st century's thorny national security problems, this new tool may be most suited for the thorniest: *LikeWar.* Just as a generation back, threat actors began to hack computer networks in what became known as cyberwar, so, too, are they now hacking social networks, driving ideas viral with real-world effect on everything from elections to terrorism. This new facet of online war has literally cost lives, from being ably used by ISIS in its rise, to fueling so much misinformation and irresponsible public health behavior during the coronavirus pandemic that the phenomenon was called an "infodemic." Given how adversaries are fusing information, narrative, influence, visuals, and psychology in this effort, it is apt that we turn to a medium that facilitates that fusion to better understand it.

Lessons Learned from *Invisible Force*

Invisible Force is ultimately a story about the power of ideas

and their simultaneous strategic influence on both small groups of people on up to entire populations. As the story asks, "As conflict slips between the digital, cognitive and physical domains, we are left to question what is an act of war?"

We certainly will not completely "plot spoil" (a difference between a memo and a narrative is that you keep the reader hooked to the end versus putting the BLUF in the executive summary, which usually ends up being the only part anybody reads). What determines the course of the multiple conflicts in the story is not a contest of brute force. It is the moment-by-moment untethering to a collective truth. When a story like *Invisible Force* takes readers from refugee camps in Atropia rocked by violent unrest to Donovian command centers to the call-in lines and chat rooms of the populism-dispensing Drip Feed, it underscores the localized strategic disorder that Army leaders will have to navigate at every level of command in the real future operating environment. From such a cauldron of complexity, we can draw forth distinct lessons from *Invisible Force* that are relevant and actionable today when it comes to shaping everything from tactics to doctrine:

Exploitable Realities

An individual's ability to differentiate between what is real and artificial is being fuzzed by the algorithmic shaping of collective realities — but not completely. As an example, the real downing of an Atropian airliner created a verifiable national moment of shock and loss, a tragedy caused by Donovian hackers intent on sowing distrust and chaos within their adversary's society. At the same time, deep fake-like videos spread throughout Atropia showed bombings in its capital and kidnappings of school children in its eastern region. In future contests of narratives, adversaries will aim to exploit small rifts between the synthetic and the real to create on-demand levels of doubt.

Broken Faith

Manufactured doubt is a recurring theme in the story. It reflects a deteriorating confidence in institutions that a generation ago would have been cornerstones of order; the parts of our society that engender trust and cooperation, and hold back coercion and, ultimately, chaos. Refugees believing vaccines are harming their children is fertile ground for targeted Donovian disinformation campaigns, while a populist American talk-show, *Drip Feed*, is the perfect medium to seed doubt about the effectiveness of the U.S. government, but doing so for ratings and profit with little regard for the institutional and societal damage it is causing.

Algorithmic Awfulness

The worst of human behavior seems to be algorithmically

amplified time and time again throughout the story by adversaries. This is a Donovian strategy that is audacious and global. It is interesting to compare the low barrier to entry of its tactics, such as deep fakes of a U.S. soldier taken hostage, to its strategic effects, inducing U.S. legislator's failure to pass technical surveillance legislation.

Software Dominance

The central and decisive technologies in the story are not the hulking physical systems of old, be they a tank or an aircraft carrier. Rather, they are the unseen zeros and ones of software in action. That they are computer code does not mean they can't have physical effect, however. Machine-learning AI, social network platforms, and hacking tools shape nearly every development throughout *Invisible Force*, which is a fitting title. These are the central tools for creating conflict, and, of course, for preventing or stemming it.

Wonder Weapons

While *Invisible Force* is an information warfare-focused story, the narrative nonetheless underscores how little hard power an adversary like the Donovians might need to wield to shape global events — and how too many of the once trustworthy and dominant conventional weapons systems may not be suited to such a future. Notably absent are many of the Army's current investment priorities, such as hypersonic strike capabilities or futuristic combat vehicles. While those may one day exist in a larger toolbox, the decisive elements for this story are pairings of unencumbered soldier initiative and AI-like software.

What Does This Mean for the U.S. Army?

There are many lessons that this project holds for the U.S. Army, but seven new "pillars of wisdom" seem to emerge from the world of *Invisible Force*.

Education: It is a new world and new ways of thinking, and sharing, are needed.

Training: Blurring lines between reality and truth requires the new skills of both digital literacy and the ability to exercise the imagination, faster than ever.

Intelligence: Know not just the enemies strengths and weaknesses, but also your own, as adversary AI algorithms are already preparing to exploit them.

Technology: The algorithms of software are more important than the physics of hardware, particularly when digital effects impact the real world.

"INTELLIGENCE: KNOW NOT JUST THE ENEMIES STRENGTHS AND WEAKNESSES, BUT ALSO YOUR OWN, AS ADVERSARY AI ALGORITHMS ARE ALREADY PREPARING TO EXPLOIT THEM.

Doctrine: When tactical/strategic surprise is moving at machine speed, doctrine must be flexible, adaptive, and, most of all, creative.

Operations: Expect that things will go wrong — really wrong — as machine learning will exploit all errors exponentially.

Leadership: Leadership will be as much about delegation as direction, trusting even more highly empowered Army servicemembers with not just tactical decisions, but decisions of strategic effect.

Seeing the Future

After reading the pages that follow, *Invisible Force* will leave you with fresh perspectives on the future of warfare, and especially its information elements. You will be able to not just step into a future conflict, but view it from the perspective of U.S. Army soldiers, their allies — and their adversaries. Perhaps more importantly, after exploring this potential future through the novel means of a graphic novel, you will also be considering new questions about not just the 'what' of tomorrow, but also 'how' to best prepare for it.

INVISIBLE FORCE

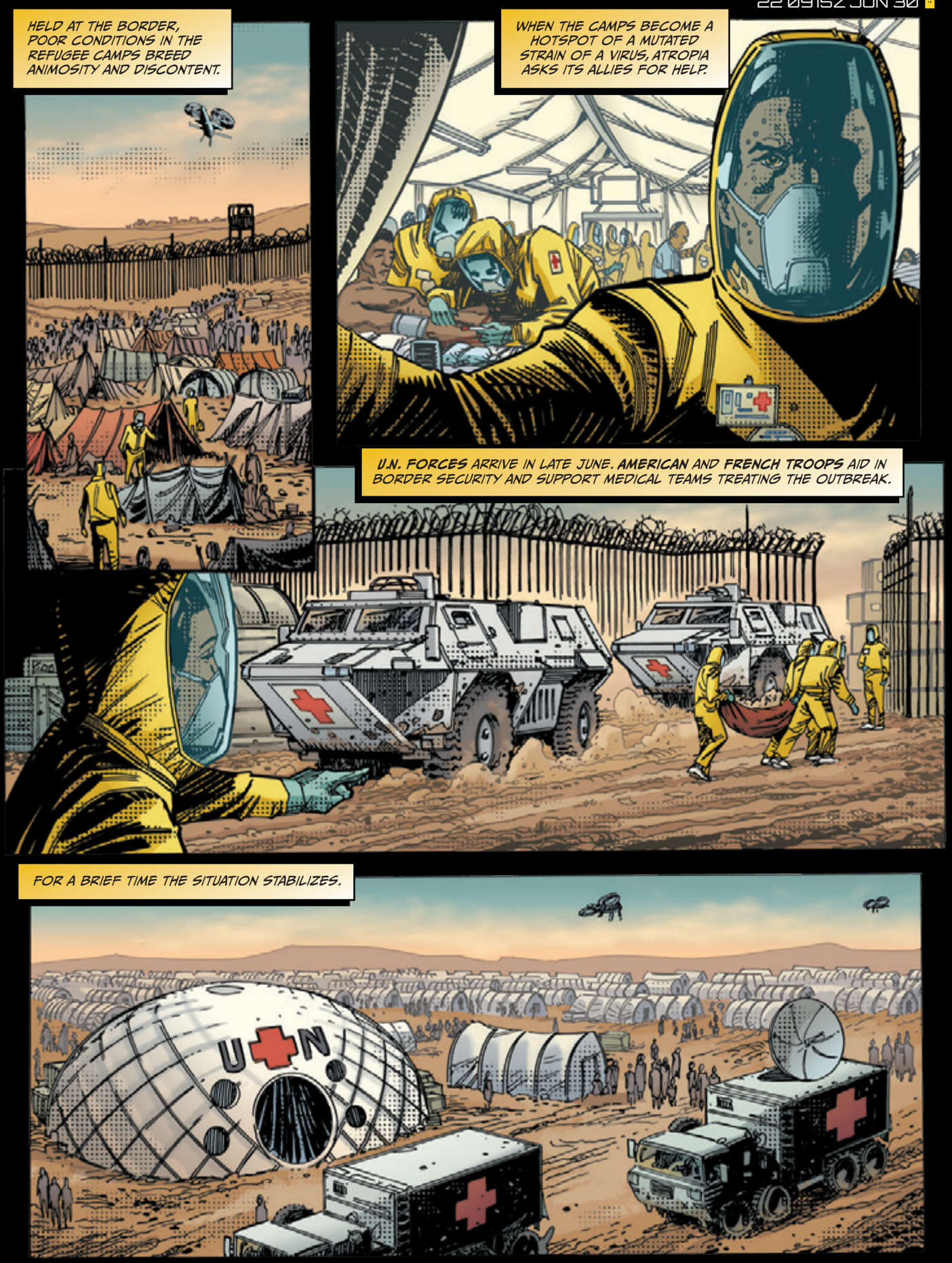
2030. Large swaths of the world are destabilized. Famine is rampant due to the aftermath of the long legacy of failed globalization. Citizens from poorer countries are migrating to escape famine, war, climate change, and lack of opportunity created by failed states. Wealthier countries, worried about resource scarcity, close themselves off to the refugees.

Amid all of this, quantum computing has been achieved, resulting in infinitely faster processing of more information than ever before. Quantum technology and a fracturing of the global alliances enable global elite to exercise control over information – resulting in a segmented Internet. Nations are now ruled by technocratic elites, some who remain committed to individual liberty and privacy, and others who extract data as a raw material from the lives of individuals, with no restrictions on its use other than profit.

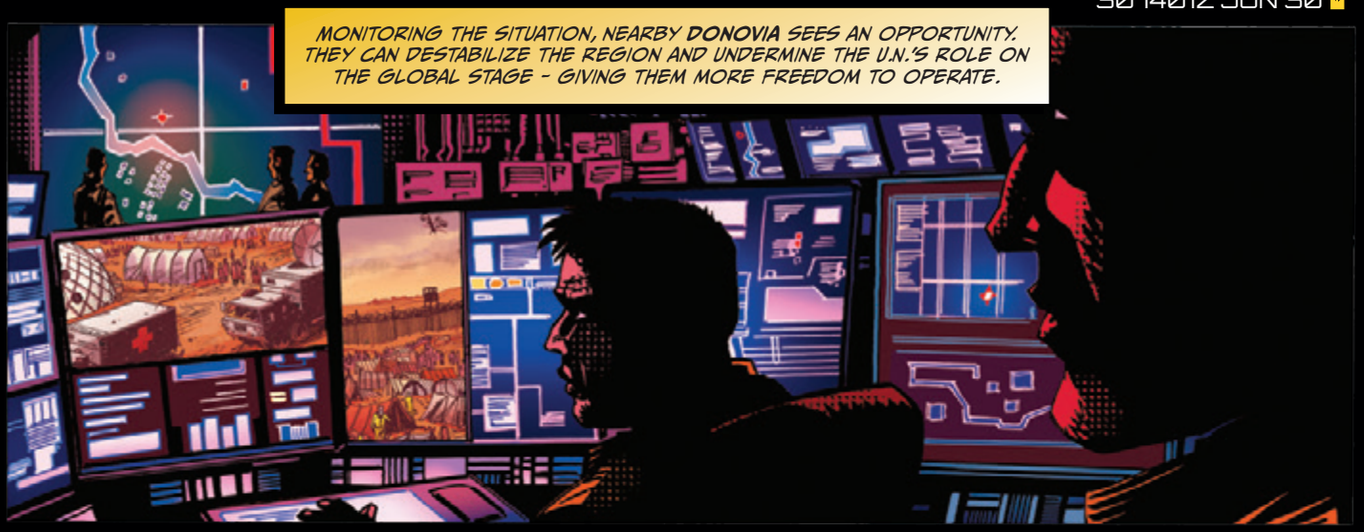
The Iron Firewall has descended between those who have adopted China's closed 5G technology and those who haven't, splitting the world into a new digital Cold War. Countries like China and Donovia use this technology to exert social control – keeping the peace within their own borders behind the Iron Firewall while stirring up trouble beyond.

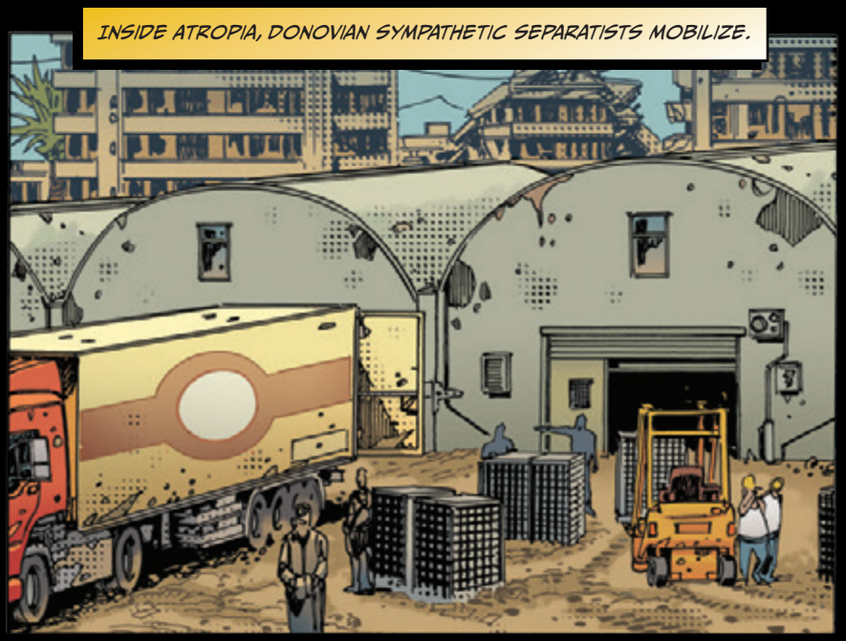
By 2030, the nature of information war has changed. Combined with new, ubiquitous technology and levels of individual customization from data extraction, people don't even realize they're being manipulated.

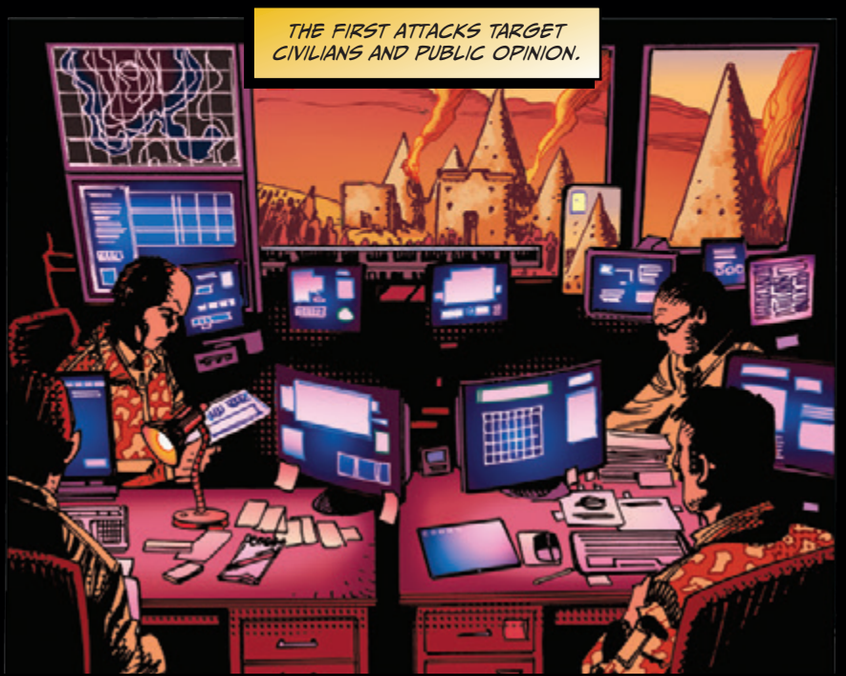

MAY 2030. AFRICAN REFUGEES FLEE A DEVASTATING SIX-YEAR DROUGHT...
...AND THE TRIBAL WARS THAT CAME ALONG WITH IT.
THE REFUGEES FLOOD ATROPIA'S SOUTHERN BORDER IN HOPES OF MOVING INTO EUROPE...
ATROPIA IS STRETCHED TO ITS LIMIT...

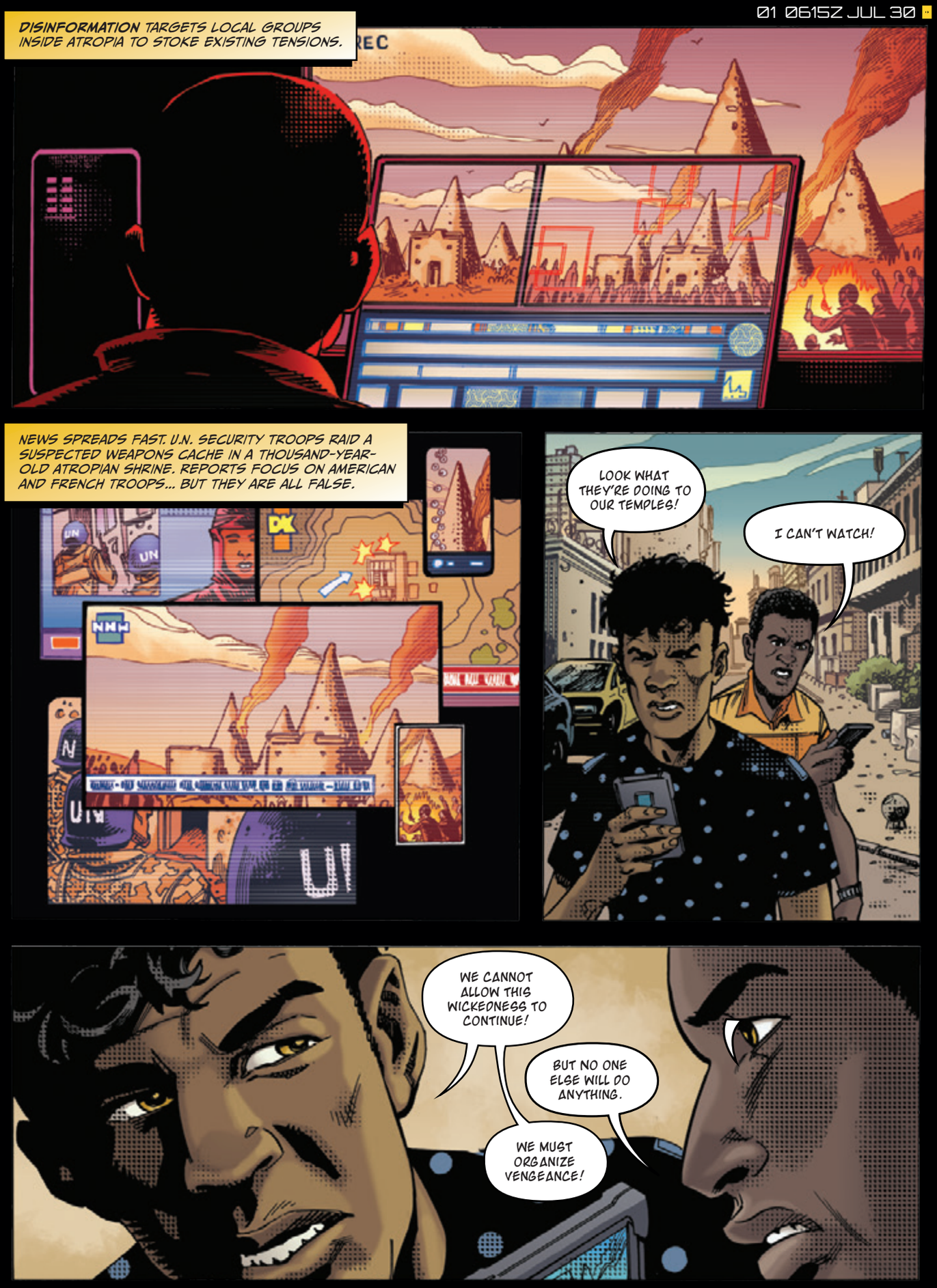

HELD AT THE BORDER, POOR CONDITIONS IN THE REFUGEE CAMPS BREED ANIMOSITY AND DISCONTENT.
WHEN THE CAMPS BECOME A HOTSPOT OF A MUTATED STRAIN OF A VIRUS, ATROPIA ASKS ITS ALLIES FOR HELP.
U.N. FORCES ARRIVE IN LATE JUNE. AMERICAN AND FRENCH TROOPS AID IN BORDER SECURITY AND SUPPORT MEDICAL TEAMS TREATING THE OUTBREAK.
FOR A BRIEF TIME THE SITUATION STABILIZES.
UN

30 1401Z JUN 30








01 0615Z JUL 30
DISINFORMATION TARGETS LOCAL GROUPS INSIDE ATROPIA TO STOKE EXISTING TENSIONS.
REC
NEWS SPREADS FAST. U.N. SECURITY TROOPS RAID A SUSPECTED WEAPONS CACHE IN A THOUSAND-YEAR-OLD ATROPIAN SHRINE. REPORTS FOCUS ON AMERICAN AND FRENCH TROOPS... BUT THEY ARE ALL FALSE.
UN
UN
DK
NMH
LOOK WHAT THEY'RE DOING TO OUR TEMPLES!
I CAN'T WATCH!
WE CANNOT ALLOW THIS WICKEDNESS TO CONTINUE!
BUT NO ONE ELSE WILL DO ANYTHING.
WE MUST ORGANIZE VENGEANCE!


OTHER CAMPAIGNS FAN THE EMBERS OF FEAR, TARGETING YOUNG MOTHERS AND PUTTING SUSPICION ON THE MEDICAL WORKERS TRYING TO CONTAIN THE VIRUS.
LET ME PASS!
NO. NO. YOU CAN'T GO TO THE CLINIC. LOOK AT WHAT THEY ARE DOING!
REPORTS SHOW MEDICAL TEAMS FORCIBLY VACCINATING BABIES, BUT THE PEOPLE SAY THAT THE VACCINE IS EBOLA.
THAT ISN'T REAL.
EVEN THOUGH IT IS A LIE AND ILLOGICAL, IT IS STILL EFFECTIVE BECAUSE PEOPLE BELIEVE.
YES IT IS! THAT IS SARAH'S SON, JACOB. ARE YOU WILLING TO RISK YOUR DAUGHTER'S LIFE?
IF WE DON'T VACCINATE, THEY WON'T LET US CROSS THE BORDER!
THEY WON'T LET YOU IN ANYWAY.

Microtargeting as Information War

***Major Jessica I. Dawson, Ph.D.**, Assistant Professor, Army Cyber Institute*

As early as 2011, the Defense Advanced Research Projects Agency (DARPA) was researching social media information sharing patterns along with social media psychological profiling.[1] Information warfare campaigns develop "insights on how best to persuade the target to change its behavior to one that is more favorable to U.S. interests. The results of [target analysis] provide the foundation for the remaining phases of the process, which in turn allows for the achievement of the objectives expressed in the supporting program(s). Analysis does not stop but continues throughout the entire operation, updating information as information is learned, the environment changes, and new [targets] are required or selected".[2] Consumer patterns help reveal additional insights about a population. By framing messaging according to "psychometric profiles," behavior modification can be achieved more reliably. "Persuasive appeals that were matched to people's extraversion or openness to experience level resulted in up to 40% more clicks and up to 50% more purchases than their mismatching or unpersonalized counterparts".[3]

The main difference between political microtargeting and military information operations is who is doing the targeting and who is the target. Substantively, the methods of analysis, information gathering, and actions used to influence behavior are all the same. The fact that one is used on perceived enemies whereas another is used to influence elections is a distinction without difference – meaningless. The goal of advertising and information warfare is the same: to influence behavior change in support of someone else's goals.

Awareness about political campaigns using social media to target potential voters has been growing since the Obama campaign first used targeted advertising to sweep into victory after the 2008 campaign.[4] Then came Brexit, followed quickly by the Trump victory, both of which caught the political class by surprise.[5] But neither of these campaigns should have caught anyone by surprise – they were merely making use of the most effective advertising platform ever created – enabled by the emergence of surveillance capitalism.[6] This new advertising capability is based not on old mass marketing techniques, but rather embedded in cultural messages[7] and targeted toward each individual with increasing accuracy.[8] The predictive power of surveillance capitalism is not only being exploited for advertising success, but increasingly harnessed for mass population control[9] in the form of information warfare, enabled by massive amounts of individually identifiable, commercially available data.

The surveillance economy information has created "a devastating weapon of mass destruction".[10] The information extracted by the surveillance economy has granted anyone with the means to access these systems "direct access to the minds and lives of guards, clerks, girlfriends…a detailed trail of personal information that would previously have taken months of careful observation to gather".[11] Individual cell phone users can be tracked using location-based information updated in real time.[12] Social media reveals what people attached themselves to and data-aggregated microtargeting has allowed it to be weaponized.[13] The sheer magnitude of information available on individuals at scale and commercially available make it critically important that researchers understand "which behaviors of large groups of people can be influenced through the application of psychological mass persuasion – both in their interest and against their best interest".[14]

The new surveillance capitalism has enabled massive information warfare campaigns that can be targeted directly at target populations at scale. Several factors have developed within the surveillance economy which, combined, create significant concern regarding the vulnerability of populations: "the rise of big data, the shift away from demographic targeting to individualized targeting, the opacity and power of computational modeling, the use of persuasive behavioral science, digital media enabling dynamic real-time experimentation, and the growth of new power brokers who own the data or social media environments".[15]

The lack of government oversight or meaningful regulation on the use of commercially available data should be significantly concerning. Recently, undergrads at Harvard were able to combine information available on the dark web with a purchased Experian database to identify nearly 1,000 high net worth individuals in Washington, D.C.. "They were able to identify 1,000 people who have high net worth, are married, have children, and also have a username or password on a cheating website. Another query pulled up a list of senior-level politicians, revealing the credit scores, phone numbers, and addresses of three U.S. senators, three U.S. representatives, the mayor of Washington, D.C., and a Cabinet member".[16]

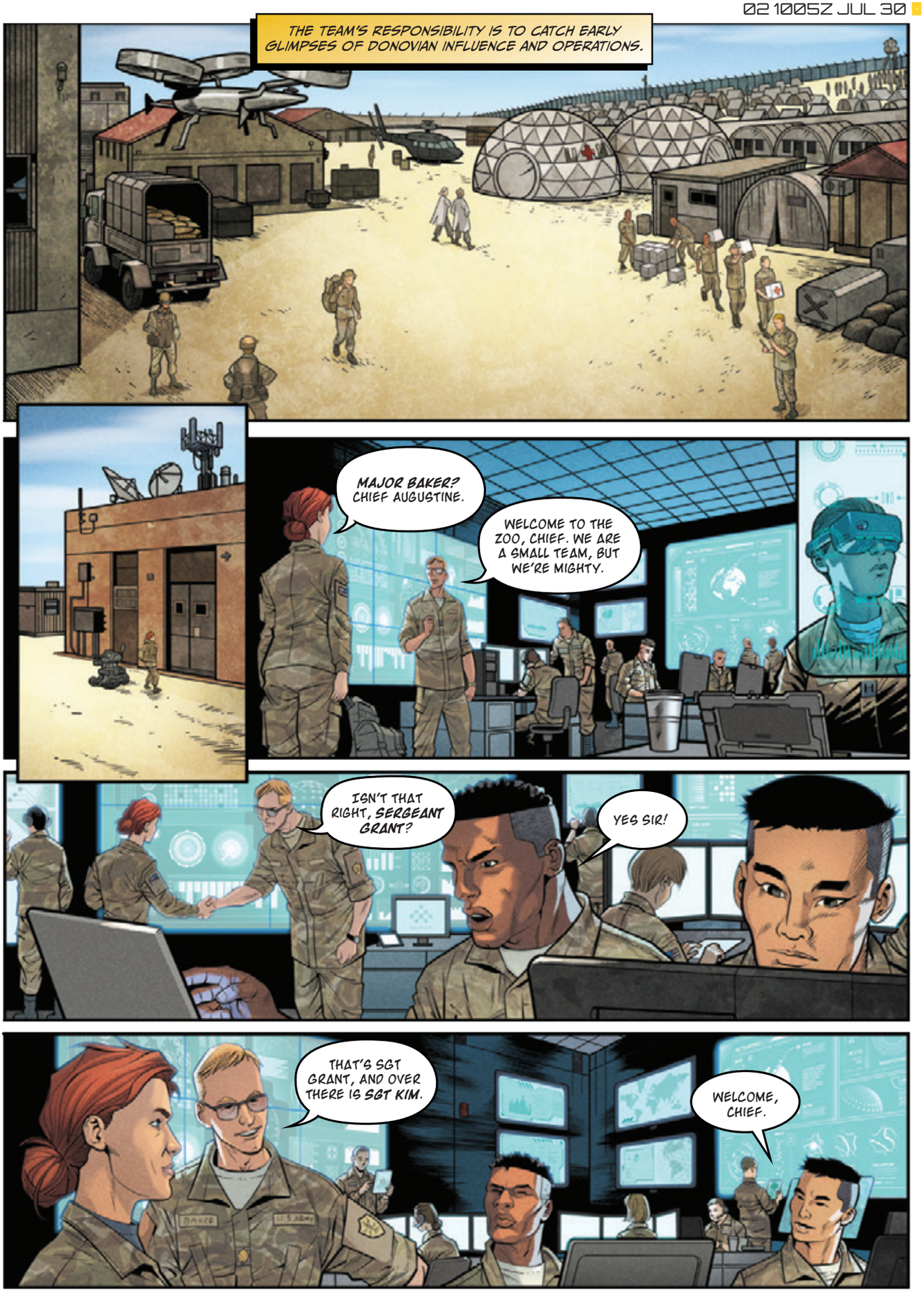
"The ability to target the trending message toward people more likely to be receptive to it reduces national security and further erodes already weakened trust in institutions."

This is not limited to college research. The United States Senate released a bipartisan, unclassified report detailing how Russian operatives targeted American election infrastructure during the 2016 election.[17] Additionally, Russian active measures used social media to exacerbate existing cultural tensions within the United States.[18] Not everyone was caught unaware: black feminists online realized some accounts were masquerading as black activists and quickly began working together to identify misinformation attempts with the hashtag #yourslipisshowing [19].

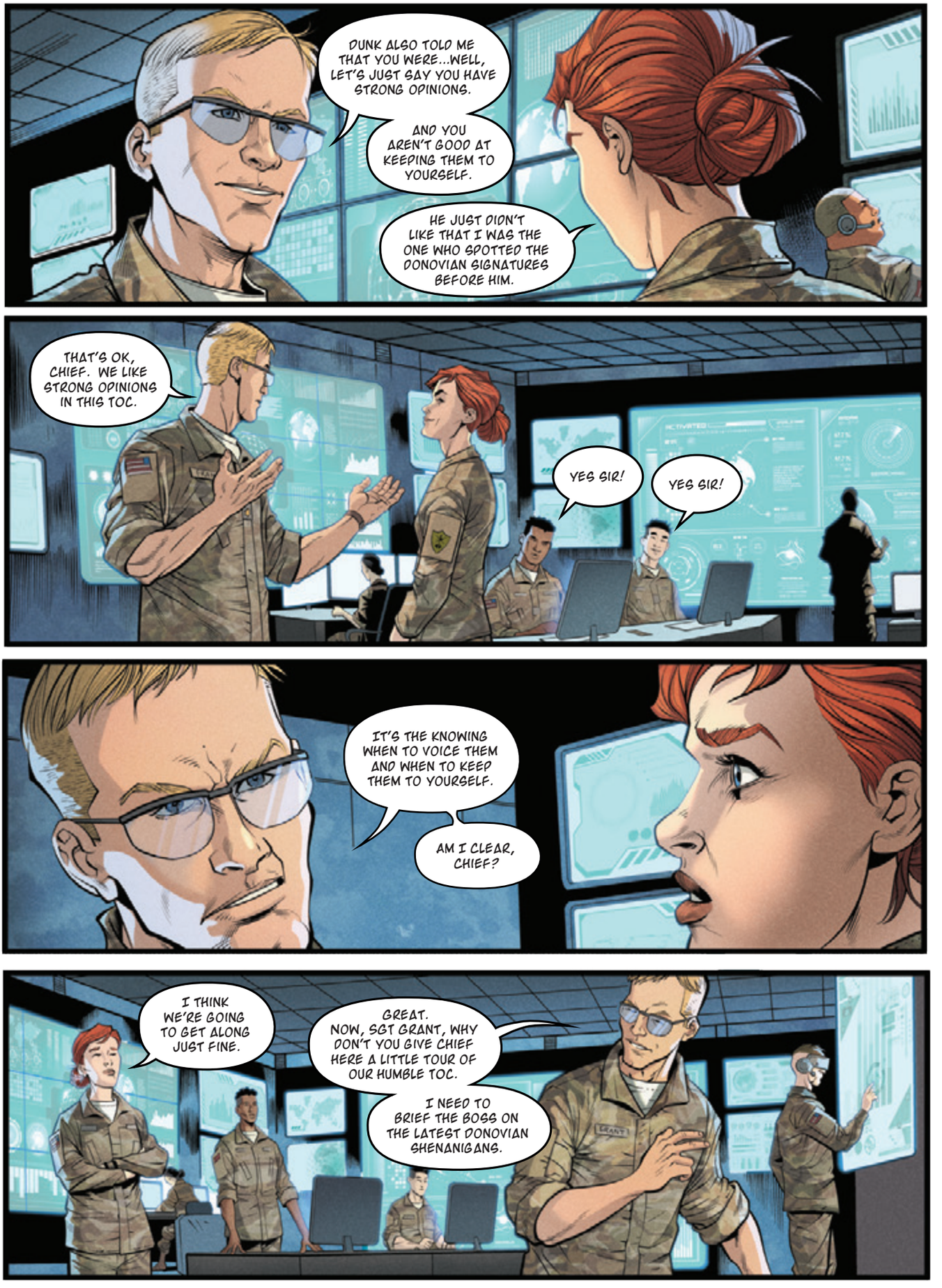
New technology has always led to massive cultural change and upheaval: the printing press freed the Bible from the grip of the Catholic Church, and was instrumental in the Protestant Reformation. Radio and news media were instrumental in the mass propaganda techniques which aided and countered the Nazi propaganda machine.[20] Fake news spreads faster than accurate news,[21] breaking down trust in institutions[22] that was already eroding over the last 40 years of growing economic inequality.[23] In today's media environment, however, "if you make it trend, you make it true".[24] The ability to target the trending message toward people more likely to be receptive to it reduces national security and further erodes already weakened trust in institutions.

KEYWORDS:
Information warfare, microtargeting, big data, social media, surveillance capitalism

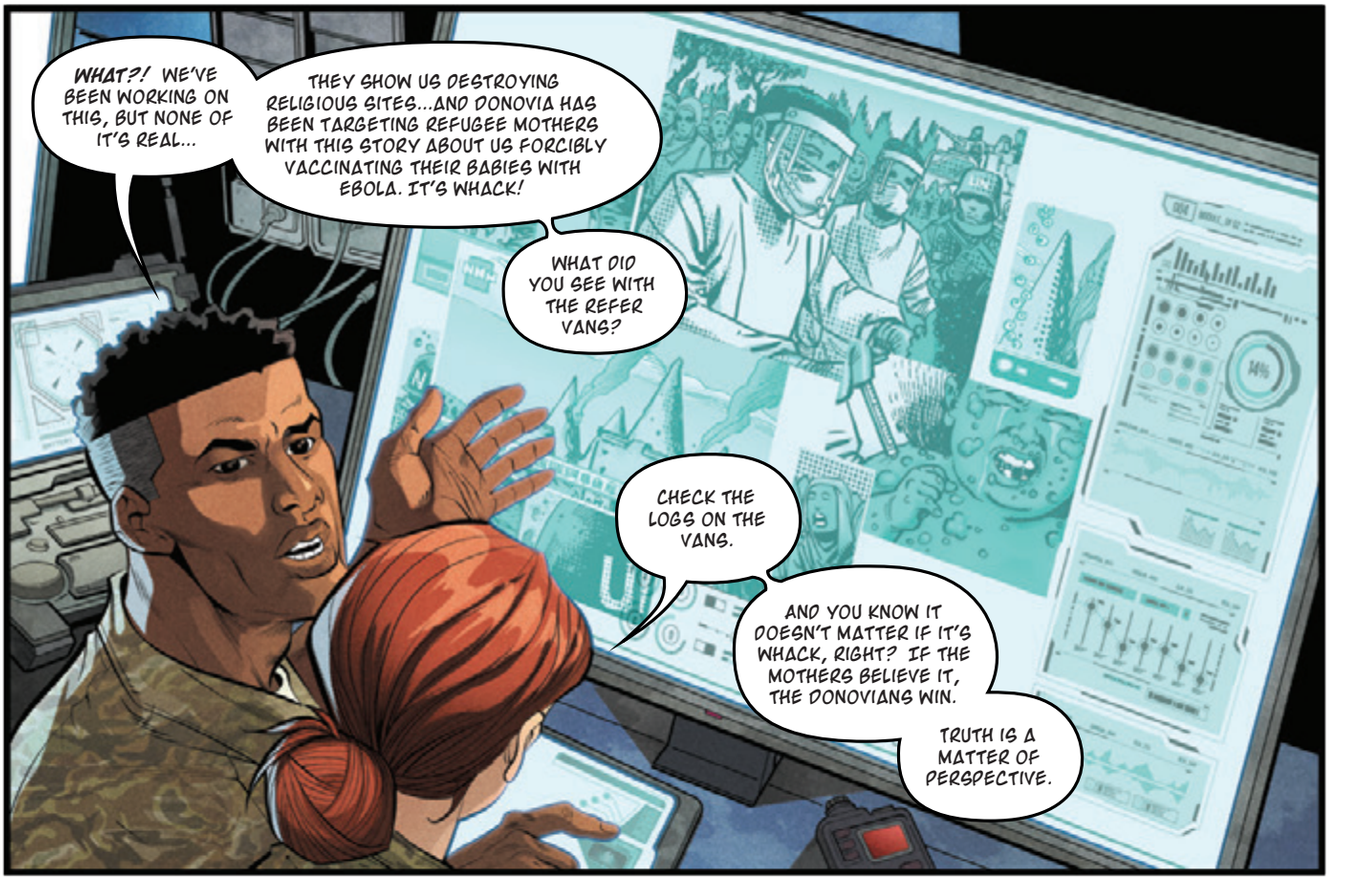

BOUND FOR THE ATROPIAN SOUTHERN BASE...
WE KNOW WHAT YOU ARE DOING! JUSTICE!
PROTECT OUR HERITAGE! ALL AMERICANS MUST LEAVE!
CHIEF WARRANT OFFICER 3 JO AUGUSTINE HAS SEEN INFORMATION WARFARE ATTACKS LIKE THIS BEFORE.
MONTHS EARLIER, DONOVIA TARGETED AN ELECTION IN ASIA, BUT HER TEAM MINIMIZED THE EFFECTS. IT WAS A SMALL WIN IN A BIG FIGHT - THE CONFLICT BEHIND THE CONFLICT.
THANKS FOR THE LIFT.
NOW, AUGUSTINE IS JOINING A SMALL FORWARD DEPLOYED INFORMATION TEAM THAT IS MONITORING DIGITAL TRAFFIC AT THE EDGE OF THE IRON FIREWALL.


THE TEAM'S RESPONSIBILITY IS TO CATCH EARLY GLIMPSES OF DONOVIAN INFLUENCE AND OPERATIONS.
MAJOR BAKER? CHIEF AUGUSTINE.
WELCOME TO THE ZOO, CHIEF. WE ARE A SMALL TEAM, BUT WE'RE MIGHTY.
ISN'T THAT RIGHT, SERGEANT GRANT?
YES SIR!
THAT'S SGT GRANT, AND OVER THERE IS SGT KIM.
WELCOME, CHIEF.


OUR FRENCH LIAISON ADELE, IS OUT WITH FARUQ, OUR TRANSLATOR, BRIEFING THE LOCAL POLICE CHIEF.
EVERYONE, THIS IS CHIEF AUGUSTINE. SHE HAS QUITE THE REPUTATION.
WELL, SIR, I DON'T KNOW IF I'D SAY...
YOUR OLD COMMANDING OFFICER, MAJ DUNCAN WAS A CLASSMATE OF MINE AT WEST POINT.
WEST POINT BUDDIES, HUH? WELL, I CAN EASILY EXPLAIN...
YEAH, DUNK TOLD ME ALL ABOUT YOU WHEN HE SAW YOU WERE HEADED OUR WAY.
HEY SGT GRANT, CHIEF AUGUSTINE HERE WAS THE ONE WHO CRACKED THE ELECTION WORK OUT EAST.
NO WAY! THAT WAS IMPRESSIVE HOW YOU TRACED IT BACK TO THEM.
SHE'S A MATHEMATICIAN AND A COMPUTER SCIENTIST. WE'RE LUCKY TO HAVE HER.
YES SIR. THAT'S GREAT.


DUNK ALSO TOLD ME THAT YOU WERE...WELL, LET'S JUST SAY YOU HAVE STRONG OPINIONS.
AND YOU AREN'T GOOD AT KEEPING THEM TO YOURSELF.
HE JUST DIDN'T LIKE THAT I WAS THE ONE WHO SPOTTED THE DONOVIAN SIGNATURES BEFORE HIM.
THAT'S OK, CHIEF. WE LIKE STRONG OPINIONS IN THIS TOC.
YES SIR!
YES SIR!
IT'S THE KNOWING WHEN TO VOICE THEM AND WHEN TO KEEP THEM TO YOURSELF.
AM I CLEAR, CHIEF?
I THINK WE'RE GOING TO GET ALONG JUST FINE.
GREAT. NOW, SGT GRANT, WHY DON'T YOU GIVE CHIEF HERE A LITTLE TOUR OF OUR HUMBLE TOC.
I NEED TO BRIEF THE BOSS ON THE LATEST DONOVIAN SHENANIGANS.


WELCOME ABOARD, CHIEF. THAT WAS SOME ACE BLOODHOUND WORK OVER IN ASIA.
THANKS. BUT YOU'VE GOT BIGGER TROUBLE HERE.
ON MY WAY IN, I SPENT SOME TIME LOOKING AT YOUR NETWORKS...
DID YOU SEE YOUR REFRIGERATION VANS WERE HACKED?
U.S. ARMY


WHAT?! WE'VE BEEN WORKING ON THIS, BUT NONE OF IT'S REAL...
THEY SHOW US DESTROYING RELIGIOUS SITES...AND DONOVIA HAS BEEN TARGETING REFUGEE MOTHERS WITH THIS STORY ABOUT US FORCIBLY VACCINATING THEIR BABIES WITH EBOLA. IT'S WHACK!
WHAT DID YOU SEE WITH THE REFER VANS?
CHECK THE LOGS ON THE VANS.
AND YOU KNOW IT DOESN'T MATTER IF IT'S WHACK, RIGHT? IF THE MOTHERS BELIEVE IT, THE DONOVIANS WIN.
TRUTH IS A MATTER OF PERSPECTIVE.


WE KNOW THAT DONOVIA HAS SPREAD ALL THIS DISINFORMATION, BUT WE'RE STUCK...
ESPECIALLY BECAUSE THE ATROPIANS ARE USING THE PROPRIETARY DONOVIAN NETWORK.
WE CAN'T DO ANYTHING!
WHO SAYS WE CAN'T? THERE'S ALWAYS A SIGNATURE. THERE'S A LOT WE CAN DO.
IT'S ALL ABOUT THE FIGHT BEHIND THE FIGHT.

Reboot

***Renny Gleeson**, Managing Director, Wieden + Kennedy, Big Innovation Group*

The new rules of conflict are being written around us by adversaries foreign and domestic; they are deploying tomorrow's weapons today, and they are winning. These new weapons systems, built from software and stories, circumvent traditional defenses and outdated processes and risk making decades of multi-trillion-dollar defense investments look like bad bets on the fighting equivalent of a twenty-first-century Maginot Line. A tech investor famously said, "software is eating the world." Our new reality is knee-deep in what's coming out the other end. *Invisible Force* illustrates that the operating system of war has gotten an upgrade, and the risks of not keeping our software up to date.

To fight and win next-gen engagement requires a full-system, full-spectrum reboot that considers how stories and software have disrupted the rules of engagement. From the hypothetical scenarios illustrated in *Invisible Force* to the practical applications of Next Generation Warfare principles in the Russian Federation's 2014 absorption of Crimea, where a story/software action practically set a new land speed record for territorial annexation, we must reimagine the threat arena. The new normal is likely to be relentless story wars interspersed with focused kinetic flare-ups; declared and undeclared wars against enemies foreign and domestic, fought with hybrid proxies, algorithms, synthetic media and adversarial narratives that exploit military/legal/cultural grey areas. How we rise to this challenge - or fail - will determine who writes the American story: adversaries or ourselves.

Any reboot should include consideration of two components: **Codespace**, the new theater of operations; and **Storyweapons**, the adversarial narratives that hijack decision spaces; as well as the new attack plain these concepts enable.

Codespace is the software-mediated reality we live now. Take a supermarket: software powers the POS system, credit card transactions, promotions, inventory management, employee scheduling, the HVAC, and opens the door to let you in and out. A supermarket without software isn't a supermarket in any real sense – it's a shed full of food going bad. Your mobile phone is a codespace interface where your interactions create raw behavioral data for predictive algorithms in a perpetual feedback loop of attention monetization. Today's "phones" aren't phones without software, they're paperweights. Codespace learns and evolves to enable seamless services and experiences; weaponized, it exploits our vulnerabilities and weaknesses to sabotage decision-making in service to adversarial objectives. Software used to live under glass, accessed through screens and interfaces; now the world is saturated with it. Life is increasingly lived through sequences of outcome-optimized, non-neutral, warning-label-free codespaces. Society has accepted the "terms and conditions", and there's no going back.

Codespace can be reconfigured to manipulate the reality experienced within it — the reality from which we create meaning and on which we base mission-critical decisions. Neuroscience has shown human perception lags reality by 80 milliseconds; next-generation mobile tech, "5G", promises sub 1 millisecond latency. Mobile augmented and virtual reality (AR/VR) tools use cameras to track eye movement and eye movement, (along with capillary dilation in the retina also captured by these cameras) reveal pre-cognitive reactions to sensory input the same way faces reveal subconscious "tells". Net, next-gen codespace will know how you feel before you do, reconfiguring in response faster than humans are equipped to perceive. If you've ever been on a date, you know humans

recalibrate interactions in real-time in response to emotional states; now our environments will, too. We've learned to be suspicious of mis- and disinformation online, but as everything goes "online", reality will be dynamically rewritten around us by algorithms that know us better than we know ourselves. And when environments attack, it's tough to shoot back.

Storyweapons are a new class of unregulated weapons systems, adversarial narratives deployed across networked codespace to hijack decision-making. They influence and actuate by hacking deep-brainstem, pre-logic cognitive systems of emotion, feeling and identity. They exploit networked connection, data, and deep stories — stories beyond truth, facts and rationality; stories that not only shape our world view but actively filter sensory input in service to it. Adversarial manipulation requires finding a story that resonates with a target's deep story to motivate action (or inaction) in service to a strategic objective. That story doesn't have to be true, it just has to be "true enough" to resonate with the target. In *Invisible Force*, adversaries instigate a kinetic response by U.S. forces and capture it on video to create a storyweapon that channels locals' cultural deep stories of honor and fairness to galvanize anti-American action.

"As everything goes "online", reality will be dynamically rewritten around us by algorithms that know us better than we know ourselves."

Current storyweapons mutate, iterate, and proliferate as fast as they can be field-deployed by humans, cyborgs, sock puppets and bots; they can be lo-fi or AI; they can take the form of "synthetic media", in deep/shallow/cheap/dumbfake 'flavors' categorized by the level of generative sophistication; they can leverage augmented audio or video content or computationally-generated alternate realities, in any media form. They can be custom-made and precision-targeted to individuals with messages optimized for actuation that maximize emotional impact and vanish after consumption; they can be deployed against entire populations, trained on hacked personal and behavioral data, and iteratively refined with brute force compute power. And that's what's available now, to anyone with a credit card.

Future storyweapons will be another thing entirely. While Lethal Autonomous Weapons Systems provide a physical world target as a function of the reality of how their kinetic systems are architected, Autonomous Storyweapons will be Deep Learning/AI/Generative Design hybrids given core objectives to execute over extended timeframes. Set loose in the wild with the freedom to iterate solutions against operational parameters, they will be codespace ghosts, a true "Invisible Force", operating below perception to manipulate decision-making and actuate targets via converged hardware, software, and experiences. They will mutate, fork, and replicate to subvert defenses and avoid identification or attribution; individual instances will be able to spin off semi-autonomous subroutines that create software families and swarms that can coalesce as needed; they'll tap consumer behavioral data sets to independently develop susceptible audience segments and computational authoring systems to deliver each of them 1:1 deep-story-resonant content; furthermore, they'll have access to resources that allow them to engage human proxies, self-finance real-world actions and purchase media amplification to lend credibility and authenticity to story lines.

You can't fight off a storyweapon with bullets, and if the intended targets are told stories they want to believe, the truth won't work, either. The only way you beat a storyweapon is with a better story – so how and where will we bring ours to life?

"Front Lines" are a "fight-the-last-war" concept: the new attack plain is global. It's estimated that ~4.6B people and between 18-26+ billion devices will be connected to the Internet by 2020. Anything that's connected has the potential to be compromised; anything — and anyone — connected to a strategic objective is an attack vector. We are the new frontline. Every mind and every wifi-connected coffeemachine. And from now on, when you go to war, your family may come with you: *Invisible Force* illustrates a situation where an adversary intent on disrupting a unit's mission interferes with a soldier's mortgage payments back home. In networked codespace, we will fight adversaries with access to criminally hacked or commercially purchased data who has built detailed profiles — including mobile telephone numbers and email — for every U.S. serviceperson and family member. Those adversaries need only twenty minutes of voice audio to train up software in anyone's tone and cadence to create synthetic audio indistinguishable from actual speech; commercially available customer service Interactive Voice Recognition (IVR) software recognizes emotional states and

> "How we rise to this challenge - or fail - will determine who writes the American story: adversaries or ourselves."

recalibrates interaction in response. Put that all together, and the reality for any forward-deployed troop, anywhere in the world, the next time your lonely child's mobile phone vibrates bedside with a call from you, when your sleepy kid picks up, late at night and alone, it may be a storyweapon on the line – an adversarial AI that speaks to your kid, in your voice. What will it say?

Storyweapons and codespace change the nature of conflict — not in some safely distant future, but right now. The front line is everywhere, in everything and every mind connected to an adversary's objectives. Armor can't stop storyweapons, bullets won't kill them, and the truth won't matter to people who want to believe the storyweapons custom-built to sabotage them. Soldiers fight battles, but stories win wars. This is a "burn the boats" moment: it's on us to develop a 21st century fighting force ready to kick ass across codespace, to reboot the software and systems critical to the defense of our people, our country, and our shared story of America.

KEYWORDS:
Storyweapons, codespace, next generation warfare, deep learning, AI, generative design

DRIP·FEED

MEANWHILE BACK AT HOME... UNREGULATED, VIRAL MARKETING, MEDIA FEEDS AGGREGATE THE NEWS FROM ATROPIA. KNOWING THAT OUTRAGE AND ANGER DRIVE UP THEIR REVENUE, ARTIFICIAL INTELLIGENCE CHAT BOTS EGG ON THE PUBLIC WITH NO SPECIFIC POLITICAL AGENDA. THEIR ONLY AGENDA IS INCREASED PROFITS — MAKING IT THE PERFECT ENVIRONMENT TO SPREAD, MUTATE, AND TAILOR DONOVIAN MISINFORMATION.

WELCOME TO **DRIP·FEED!** I'M YOUR HOST AND CHIEF-CLEVERBOT, **TAD LUMLEY.**

SO, TONIGHT'S TOPIC IS...WHY THE HOLY HECK ARE WE STILL INVOLVED WITH THE U.N.?

HAVE YOU SEEN THE REPORTS COMING OUT OF ATROPIA? THEY DON'T WANT US THERE! I WANNA HEAR WHAT YOU THINK!

WE'VE GOT OUR FIRST AGITATOR! LAY IT OUT FOR US, **CHERYL!**

15%

Yeah, I think it's just terrible! I'm shocked! There is a new virus out of control over there! Why are our troops in Atropia when we've got so many problems here at home? Manufacturing is dead and I'm unemployed!

INFLUENCER POINTS:
1,759
CHERYL

@SeenThruGlass

Been a hectic day and only just catching up on global news.. at what point do we grab shotguns and a hummer?
#EndOfTheWorld

NEXT, WE HAVE **MATT.** YO, WHAT'S YOUR BROPINION?

75%

This Atropia deal is disturbing. Why we are wasting so much money and American blood on foreigners? I don't think that Congress has any idea what it's doing. It makes me question if the government is really working for "we the people" or if they only care about their wealthy donors.

SPONSORS

@Sallysass

Have you seen this fresh ridiculousness! I can't believe this just happened!

INFLUENCER POINTS:
3,612
MATT

THAT'S MIND BOGGLING THERE, MATTY BOY — SOME REAL RATIONAL IGNORANCE!

DONOVIA INFLUENCES AMERICAN OPINION AND UNDERMINES SUPPORT FOR ATROPIA. THEY FILL THE MEDIA WITH TAILORED DISINFORMATION AND INCENDIARY VIEWS, STOKING BOTH SIDES, SEEDING DOUBT, AND SCATTERING DISSENT ON ALL SIDES.

DOF LIVE

WHO'S GOING NEXT? **CHARLES**...DIVE IN!

65%

When we've got American soldiers desecrating holy sites, we've lost the moral authority to intervene around the world. Clearly, we've got a failure in leadership at the very top! We need to stand up and unite to make a change!

EXCLUSIVE NEWS INTERNATIONAL

THIS IS ALL VERY UNSPIRATIONAL SO FAR...

INFLUENCER POINTS: 12,587 CHARLES

YOUR TURN, **SALLY**! GIVE US SOME TRUISM!

65 CORPS

@NinjViews

What do you nknow?! We can either be like an army of ants-organized/heading in the same direction...or we can scatter—running in all directions #AmyAntz

EXCLUSIVE NEWS INTERNATIONAL

5%

My husband was just fired because his employer tracked him going to a protest rally! I guess his foreign bosses don't like free speech! Why aren't we talking about that?

INTERESTING, SALLY. BUT I'M AFRAID YOU'VE GOT NO SUPPORT.

QUIT PROCASTIBATING PEOPLE! GIVE ME SOMETHING STOKEWORTHY!

@SalutionSong

People who don't care about data privacy should be worried about huge behavioural databases that can fuel dark ads and make Donovian corporations very rich. #dataprotection

INFLUENCER POINTS: 536 SALLY

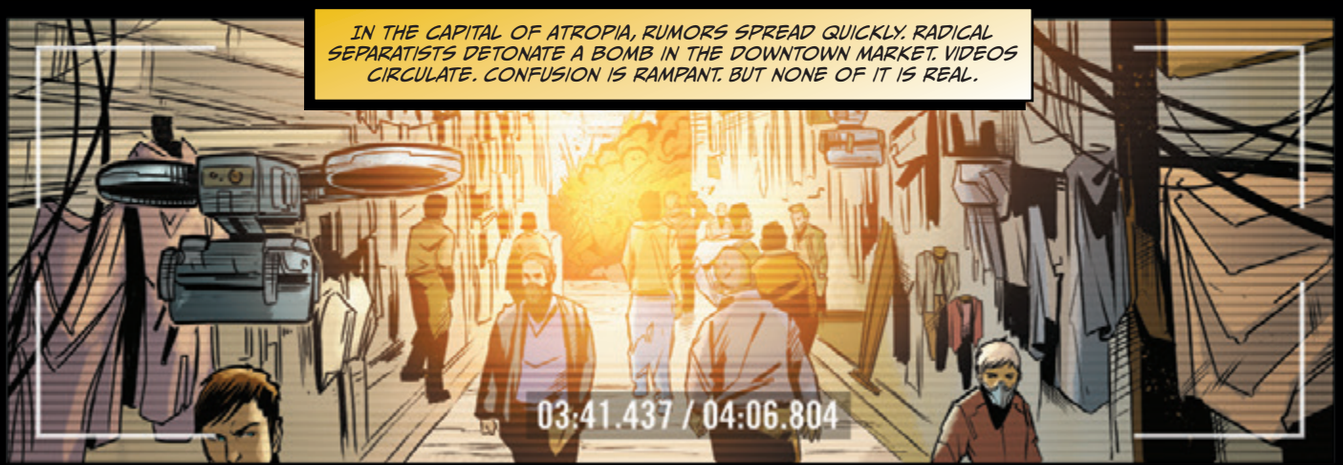
BIT BY BIT, DONOVIA ERODES TRUST IN THE AMERICAN GOVERNMENT AND CREATES INSTABILITY.

THE INITIAL INFORMATION WARFARE ATTACKS WERE JUST A TEST. THE REAL OFFENSIVE STARTS WHEN DONOVIA LAUNCHES A SERIES OF COORDINATED ATTACKS THEY HAD BEEN PREPARING FOR YEARS.

05 0715Z JUL 30

THEY CALL IT **GRAY WEDNESDAY.** IT IS THE FIRST OFFENSIVE OF ITS KIND - USED TO THROW ATROPIA INTO CHAOS AND SHAKE THE WORLD. BUT NOT ONE SHOT IS FIRED.

IN THE CAPITAL OF ATROPIA, RUMORS SPREAD QUICKLY. RADICAL SEPARATISTS DETONATE A BOMB IN THE DOWNTOWN MARKET. VIDEOS CIRCULATE. CONFUSION IS RAMPANT. BUT NONE OF IT IS REAL.



ON THE SAME DAY, **28 STUDENTS** FROM AN ALL-GIRLS SCHOOL IN EASTERN ATROPIA ARE KIDNAPPED. THE PUBLIC IS SHOCKED. THIS, TOO, IS FALSE.


EVEN WHEN VIDEOS OF THE GIRLS RETURNING FROM THEIR FIELD TRIP CIRCULATE, PEOPLE DON'T BELIEVE IT. ATROPIANS CALL OUT FOR THEIR MISSING GIRLS.
AT THE END OF THE DAY, THE DOWNING OF ATROPIAN FLIGHT 435 CATCHES THE WORLD'S ATTENTION.
ATROPIAN AIR
CONFLICTING REPORTS BLAME A SOFTWARE GLITCH OR MECHANICAL MALFUNCTION.
THEN A COCKPIT VIDEO IS LEAKED FROM FLIGHT 435. IT STREAMS AROUND THE WORLD. IT IS A FAKE.
THIS ISN'T ME! IT WON'T PULL UP... WHAT DO I DO?!
06:11.127 / 08:16.358
THE DONOVIAN OFFENSIVE ON ATROPIA IS JUST BEGINNING...

Everything is a Computer, and Computer Security is Everything Security

***Bruce Schneier**, Security Technologist and author [www.schneier.com]*

Everything is becoming a computer. Your smartphone isn't a phone; it's a small portable computer that happens to make phone calls. Similarly, your refrigerator is a computer that keeps things cold. And your microwave is a computer that makes things hot. An ATM is a computer with money inside. Your car is a computer with four wheels and an engine. Actually, it's a 100-computer distributed system with four wheels and an engine.

This is happening throughout society, from the personal to the large. A power plant is a computer that happens to produce energy.

This is the Internet of Things, and what it means is that everything that's relevant about computer security becomes relevant to everything, everywhere. The same bugs and vulnerabilities that have plagued our more traditional computers are about to plague everything, everywhere. We'll experience the same insecurities, the same criminal hacks, the same data thefts, and the same nation-state operations. The difference is that these computers affect the world in a direct physical manner.

Automation, autonomy, and physical agency bring new dangers. What separates traditional computers from the Internet of Things is what the computers are doing and what they're attached to.

There's an old concept from computer security called the CIA triad. That stands for confidentiality, integrity, and availability: the three properties computer security is supposed to provide. Most of the time, when there's a computer security story in the news it's a confidentiality story. Think of Equifax, the Office of Personnel Management, Facebook and Cambridge Analytica. When there's a confidentiality breach, you've lost control of your data.

Those are serious security vulnerabilities. But when it comes to computers that affect the world in a direct physical manner, the integrity and availability threats are much worse than the confidentiality threats. Their effects are much greater, because there's real risk to life and property. I am concerned if someone hacks a hospital and steals my confidential medical records, but I am much more worried if they can change the record of my blood type. That's a data integrity attack. I am concerned if someone hacks my car and eavesdrops on my conversations, but I am alarmed if they remotely disable the brakes. That's a data availability attack — the hacker renders the controls unavailable.

Think of cars, medical devices, drones, weapons systems, thermostats, power plants, smart city systems. There is a fundamental difference between crashing your computer and losing your spreadsheet data and crashing your pacemaker and losing your life. And it could be the exact same CPU, operating system, applications software, vulnerability, attack tool, and attack. The only difference is what the computer is doing and what it's attached to.

It's all connected. We've already seen vulnerabilities in consumer devices used to launch distributed denial-of-service attacks against critical Internet infrastructure. Criminals have shut hospitals down with ransomware, and researchers have demonstrated ransomware against cars and home

thermostats. Today, the security of your webcam, refrigerator, and digital video recorder affect national security.

Fixing this requires changes in both technology and policy. But as overall strategy, I offer two principles. First, defense must dominate. It is impossible to build systems that are secure when the good guys use them and can be used for surveillance when the bad guys use them. We either design the systems to be secure, even though that means we lose the ability to spy on our enemies, or we design them to be open to surveillance, even though that means we will be vulnerable as well. Because these systems are so critical, the second option is not acceptable. We must design them for security. Every elected official, police officer, nuclear power plant operator, election official, and CEO has a smartphone. We can't afford to put backdoors in them.

"We need systems that monitor other systems, and restore security when lost."

Second, we must design resilience into these systems. We need to assume insecurities, and design systems that remain secure regardless. We need to build in security measures like defense in depth, compartmentalization, and redundancy. We need to avoid single points of failure, and design systems to fail safely and security. We need systems that monitor other systems, and restore security when lost.

There's real research to be done, similar to the research that gave rise to the Internet. The Internet was created to answer this question: Can you build a reliable network out of unreliable parts? This leads to a similar but very different question: Can you build a secure network out of insecure parts? The answer isn't obviously yes, but it isn't obviously no, either.

Both of those principles will be hard. They require the political will to defend against threats that have not yet materialized. That's a very hard thing to ask for right now. But without it, we will forever be playing catch-up in security. And as computers permeate every aspect of our lives, from the personal to the national, that will become harder to sustain.

Bruce Schneier is a security technologist and author. His most recent book is *Click Here to Kill Everybody*: Security and Survival in a Hyper-Connected World. His writing can be found at www.schneier.com.

Click Here to Kill Everybody: Security and Survival in a Hyper-connected World (W. W. Norton & Company, 2018)

https://www.schneier.com

KEYWORDS:

Privacy, computer security, surveillance, cryptography, encryption, vulnerabilities


IN THE DAYS AFTER GRAY WEDNESDAY, THE SUBSEQUENT DONOVIAN DISINFORMATION SPRAY ONLY AMPLIFIES THE UNCERTAINTY. DURING THE CONFUSION, THE SOUTHERN BASE SCRAMBLES TO UNDERSTAND THE REPERCUSSIONS AND MAINTAIN ORDER.
U N
UNABLE TO DEAL WITH THE TURMOIL RESULTING FROM THE ATTACKS, ATROPIA REACHES OUT TO THE U.N. AND REQUESTS MORE SECURITY SUPPORT.
FUELED BY UNCERTAINTY, THE ATROPIAN PUBLIC BLAMES THE U.N. FOR GRAY WEDNESDAY.
FALSE REPORTS CIRCULATE THAT THE SEPARATISTS ARE USING THE REFUGEE CAMP TO HIDE OUT. THE INCREASED MILITARY PRESENCE IN THE CAMPS UNLEASHES A GLOBAL HUMAN RIGHTS OUTCRY.


OVERWHELMED, LOCAL LAW ENFORCEMENT STRUGGLES TO KEEP ORDER.
GOOD MORNING, CHIEF.
WHAT DO YOU WANT ME TO DO? I DON'T HAVE ENOUGH MEN!
THE NETWORK IS DOWN. I CAN'T EVEN COMMUNICATE WITH THE PUBLIC!
HEY, FARUQ. ARE YOU JUST COMING FROM THE CLINIC? HOW ARE THINGS?
NOT GOOD. THE FAMILIES DON'T TRUST THE VACCINE OR THE DOCTORS. ONE OF THEM WAS ATTACKED LAST NIGHT.
THAT'S TERRIBLE. ARE THEY GOING TO BE ALRIGHT?
I HOPE SO, BUT I DONT THINK ANYONE IS GOING TO TRUST EACH OTHER FOR A LONG TIME.
I CAN'T BELIEVE THIS!
EXCUSE ME. SORRY, CHIEF. FARUQ.
KIM
US ARM
WHAT THE TEAM DOESN'T KNOW IS THAT THE ATTACKS ARE NOT JUST LIMITED TO ATROPIA.


DONOVIA HACKS INTO THE AMERICAN BANKING AND SUPPORT INDUSTRIES, TARGETING SERVICE MEMBERS AND THEIR FAMILIES.
WHAT'S WRONG WITH KIM?
HIS DAUGHTER'S SCHOOL KEEPS SENDING HIM ALERTS THAT HER TUITION ISN'T PAID AND HIS WIFE IS FREAKING OUT...
THEY ARE GOING TO KICK HIS DAUGHTER OUT.
SOUNDS LIKE A BANK GLITCH.
BANKS DON'T GLITCH. SOMETHING'S UP. SIMPSON IN OPS SAID HIS BANK WASN'T PROCESSING HIS MORTGAGE PAYMENTS.
DONOVIA'S GOAL IS TO DISTRACT AND DISORIENT - UNDERMINING SOLDIERS' ABILITY TO CARE FOR THEIR FAMILIES AND TRUST THEIR SUPPORT NETWORKS.
SORRY ABOUT THAT. I DON'T KNOW HOW MANY TIMES I NEED TO TELL THEM...NEVER MIND...
MY POOR WIFE DOESN'T HAVE TIME FOR THIS!


VERIFYING THE TRUTH HAD BECOME DIFFICULT, BUT CONVINCING THE PUBLIC OF THAT TRUTH WAS NEARLY IMPOSSIBLE.
DID YOU SEE THE NEW RESPONSE ON THE YOUNG GIRLS FROM GRAY WEDNESDAY?
PEOPLE STILL THINK IT'S REAL.
I WANT YOU TO DO A REVERSE VIDEO SEARCH ANALYSIS OF ALL THE FEEDS.
SOME OF THE OPEN SOURCE INTELLIGENCE SAYS THE VIDEOS ARE REAL, BUT OF DIFFERENT GIRLS FROM AN ATTACK MONTHS AGO.
MY PEOPLE ARE DYING!
I DON'T HAVE ENOUGH MEN TO GET THE WORD OUT AND NOW THE NETWORK IS DOWN! HOW AM I SUPPOSED TO GET THOSE YOUNG MOTHERS TO TRUST THE DOCTORS?
YOU HAVE TO FIX IT!
CHIEF TAHIRI, WE CAN'T FIX IT. IT'S NOT OUR NETWORK.
IT WAS BUILT ON A DONOVIAN BACKBONE. WE CAN'T EVEN TOUCH IT.
THEY ALL THINK THAT THE VACCINE IS POISON!
HE'S RIGHT.
EXPLAIN.
REMEMBER I SAID THE REFER VANS WERE HACKED?
TO KEEP THE VACCINE GOOD IT HAS TO BE STORED IN A REFRIGERATOR BETWEEN 35 AND 46 DEGREES.


WHAT DOES THAT HAVE TO DO WITH THE REFER VAN'S GETTING HACKED?
I DID SOME DIGGING IN THE LOGS OF THE VANS CONNECTED FRIDGES...
ACTIVATED
BAKER
LOOK HERE. SOMEONE GOT ACCESS TO THE THERMOMETER CONTROLLERS AND RAISED THE TEMPERATURES SO THAT THE VACCINES SPOILED.
BUT SEE... THEY DID IT AT NIGHT WHEN NO ONE WOULD NOTICE...
...AND THEY DISABLED THE ALERT SYSTEM. ALL THE VACCINES THAT WERE IN THOSE REFER VANS ARE BAD.
THE DOCTORS AREN'T INJECTING THOSE KIDS WITH POISON, BUT THEY ARE INJECTING THEM WITH A ROTTEN VACCINE.
SO THOSE REPORTS AREN'T 100% FALSE.
THAT'S WHAT MAKES THEM MORE DANGEROUS...
IF A DISINFORMATION ATTACK IS 90% FALSE BUT 10% TRUE, IT'S MUCH MORE EFFECTIVE.

Post-Truth

***Lee C. McIntyre, Ph.D.**, Philosopher, author, educator, leemcintyre@rcn.com*

"Post-Truth" is a tactic that can be used in disinformation campaigns, to muddy the waters and demoralize people into thinking that there is no basic agreement about facts. This tactic is often used by authoritarian leaders — and those who emulate them — to try to get a population to become cynical about whether "truth" even exists. In the absence of facts, a group may turn to their own "strong leader" to tell them what is true and what is false. In this way, post-truth can undermine democratic values, along with the discovery of truth itself.

Another important aspect of post-truth, however, is its potential effect on group decision making, where there might be disagreement among the stake-holders about what the facts even are.

It is important to remember, however, that post-truth is embedded in the intentional attempt to subordinate reality to ideology. As such, it trades on information that is created in bad faith, as a means to manipulate other people. In a group setting of allies —where we might reasonably assume good faith by our fellow decision makers, who are just trying to solve a problem along with us — is post-truth really a worry? Probably not. Post-truth is not synonymous with disagreement over facts. It is, instead, the intentional creation of confusion over the facts for the purpose of ideological manipulation.

In a group setting where there is disagreement over facts — but no suspicion of bad intent — a better way to facilitate decision making might be to have a "designated skeptic" who questions our assumptions about what we take to be the facts, solely for the purpose of playing devil's advocate. This concept was employed in the early part of the 21st century by U.S. Army General David Petraeus in training new officers at Fort Leavenworth, Kansas, as a means to combat the sort of "group think" that can pervade decision making in any hierarchical setting. As Petraeus put it, "the truth is not found in any one school of thought, and arguably it's found in discussion among them. This is a flexibility of mind that really helps you when you are in ambiguous, tough situations."

In a post-truth environment, the role of a designated skeptic might therefore be to make clear that the role of this person is NOT to manipulate others or create chaos, but instead merely to question whether we know what we think we do. It is, in short, a GOOD thing to question whether we know the facts before making a decision. Disagreement is not a bad thing, since it can help us to discover crucial information.

Post-truth is a danger only when one has reason not to trust one's fellow decision makers — where they are under suspicion of intentionally trying to create discord or manipulate the political environment.

Outside this, disagreement is to be welcomed and even cultivated, as a means of being certain that we are not overlooking our own biases, and therefore unintentionally putting ideology ahead of facts because we are too certain that we are right.

Further Reading:

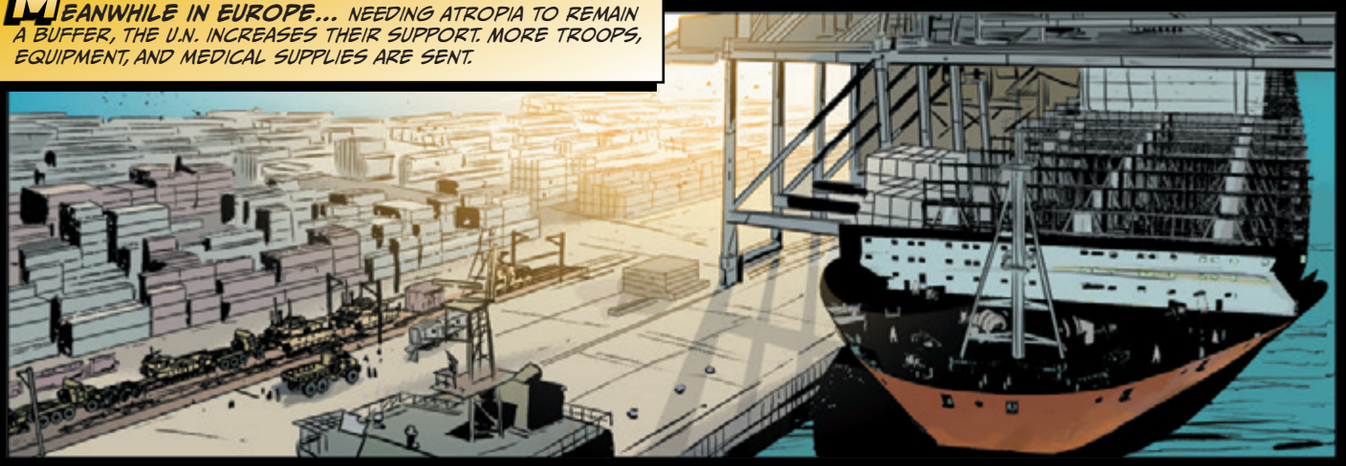
1) Lee McIntyre, Post-Truth (MIT Press, 2018)

2) Julian Barnes, "An Open Mind for a New Army" U.S. News and World Report (October 31, 2005). https://web.archive.org/web/20100825144230/http://www.usnews.com/usnews/news/articles/051031/31petraeus.htm

KEYWORDS:

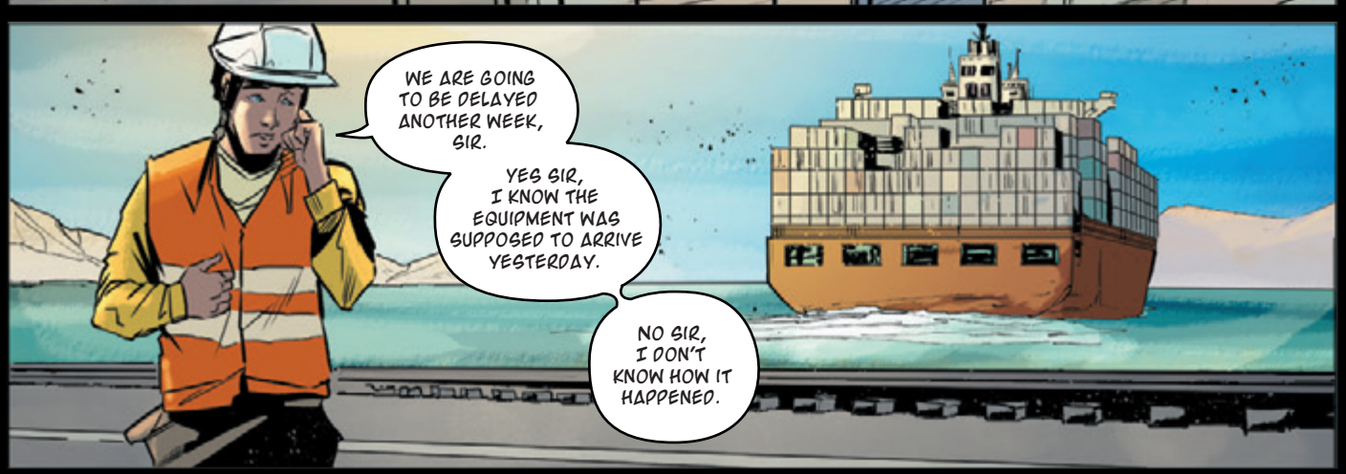
Disinformation, cyber, warfare, geopolitics, international relations

MEANWHILE IN EUROPE... NEEDING ATROPIA TO REMAIN A BUFFER, THE U.N. INCREASES THEIR SUPPORT. MORE TROOPS, EQUIPMENT, AND MEDICAL SUPPLIES ARE SENT.

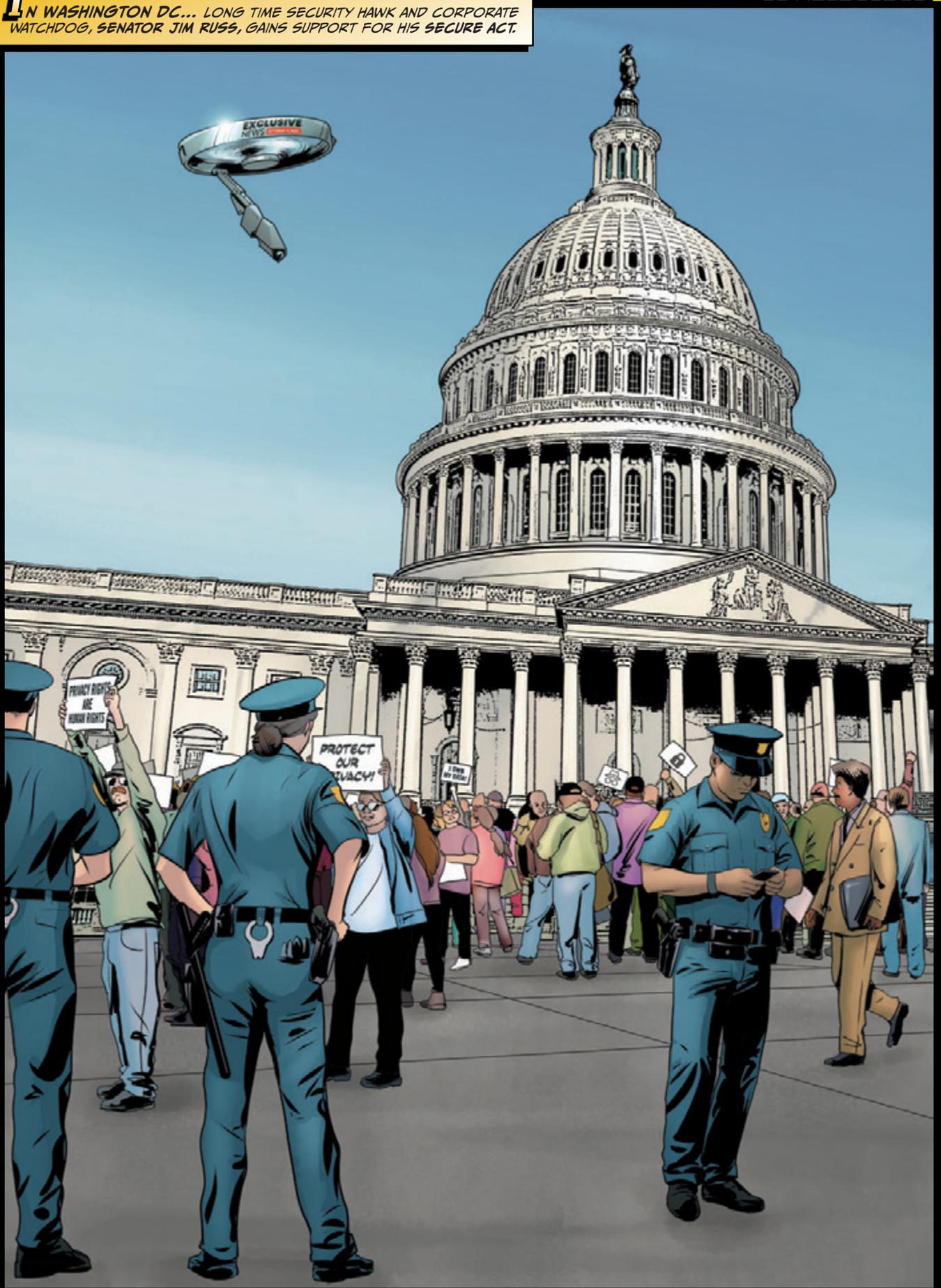


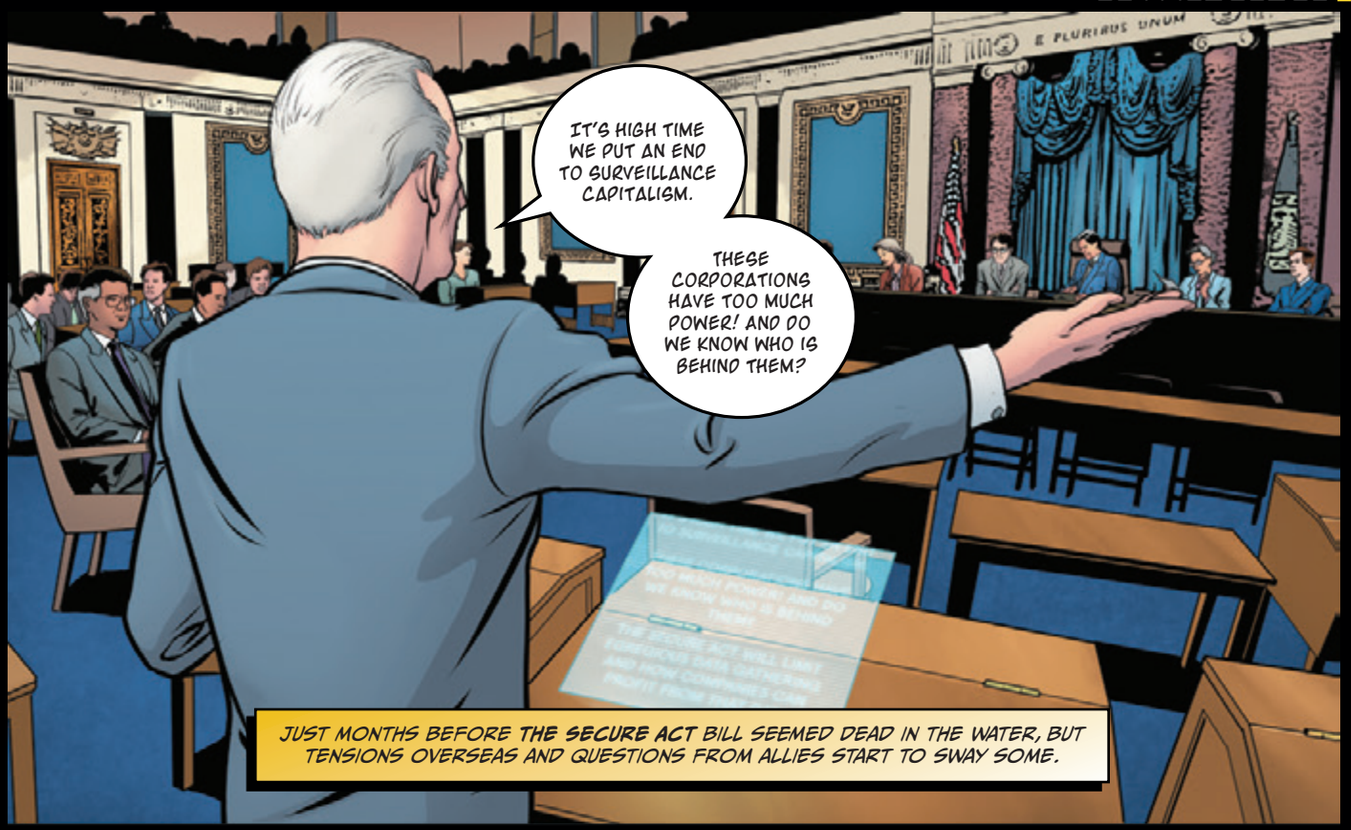
DONOVIAN MEDDLING AMPLIFIES A LOCAL TRADE DISPUTE AT A KEY PORT...

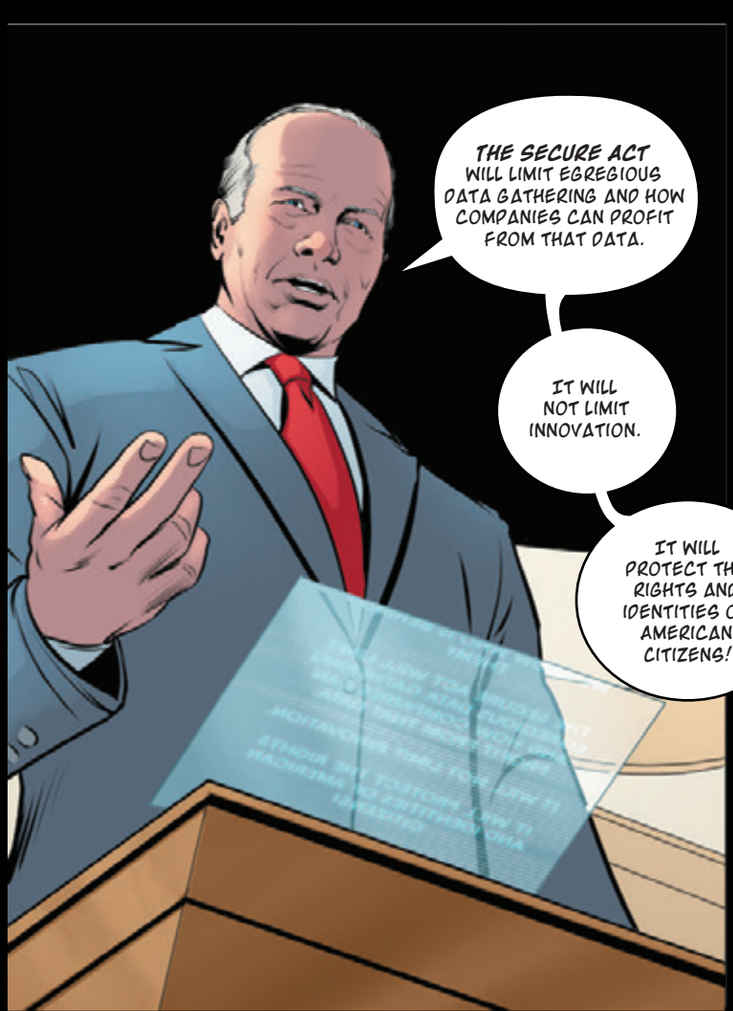
LEAVING IT UNDERSTAFFED AND VULNERABLE TO A CYBER ATTACK, THE SUPPLY CHAIN SLOWS TO A CRAWL.




MEANWHILE BACK IN AMERICA...
DID YOU SEE THIS REPORT?
TURNS OUT, ALL THESE CORPORATIONS ARE MONITORING EVERYTHING WE DO...
LOCATION, AUDIO, CREDIT, BIOMETRICS, EVERYTHING!
EXCLUSIVE NEWS
IT'S WORSE. THEY ARE USING THAT COLLECTED DATA AGAINST US.
THESE EMPLOYEES WERE FIRED BECAUSE THEY WENT TO A PROTEST RALLY.
TURNS OUT, THEIR COMPANY WAS TRACKING THE BIO-DATA ON THEIR PHONES.
DONOVIAN-FINANCED COMPANIES WORK BEHIND THE SCENES TO EXERT INFLUENCE OVER THE PUBLIC DEBATE.
DISCUSSES THE SECURE ACT
EXCLUSIVE NEWS
HEY! HERE'S THAT SENATOR WHO'S TRYING TO DO SOMETHING ABOUT IT.
HE'S CALLING IT THE SECURE ACT.

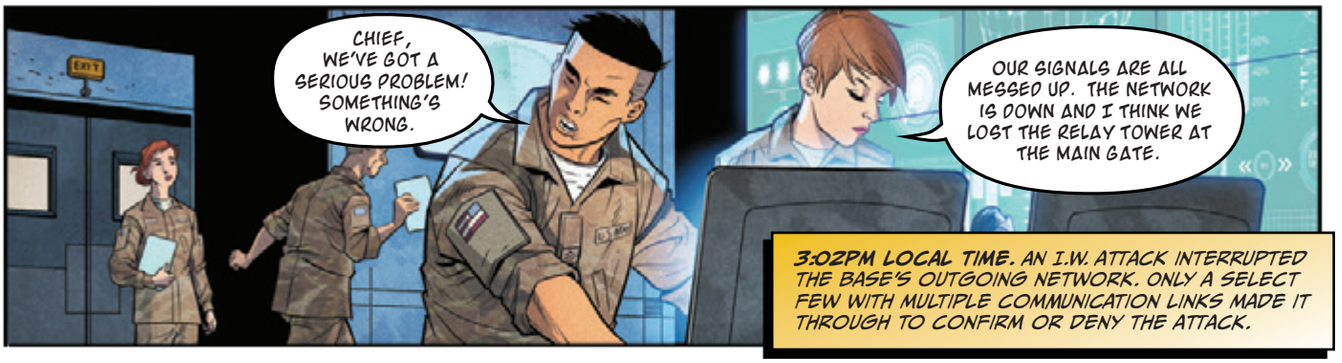

IN WASHINGTON DC... LONG TIME SECURITY HAWK AND CORPORATE WATCHDOG, SENATOR JIM RUSS, GAINS SUPPORT FOR HIS SECURE ACT.
EXCLUSIVE NEWS
PRIVACY RIGHTS ARE HUMAN RIGHTS
PROTECT OUR PRIVACY!


E PLURIBUS UNUM
IT'S HIGH TIME WE PUT AN END TO SURVEILLANCE CAPITALISM.
THESE CORPORATIONS HAVE TOO MUCH POWER! AND DO WE KNOW WHO IS BEHIND THEM?
JUST MONTHS BEFORE **THE SECURE ACT** BILL SEEMED DEAD IN THE WATER, BUT TENSIONS OVERSEAS AND QUESTIONS FROM ALLIES START TO SWAY SOME.

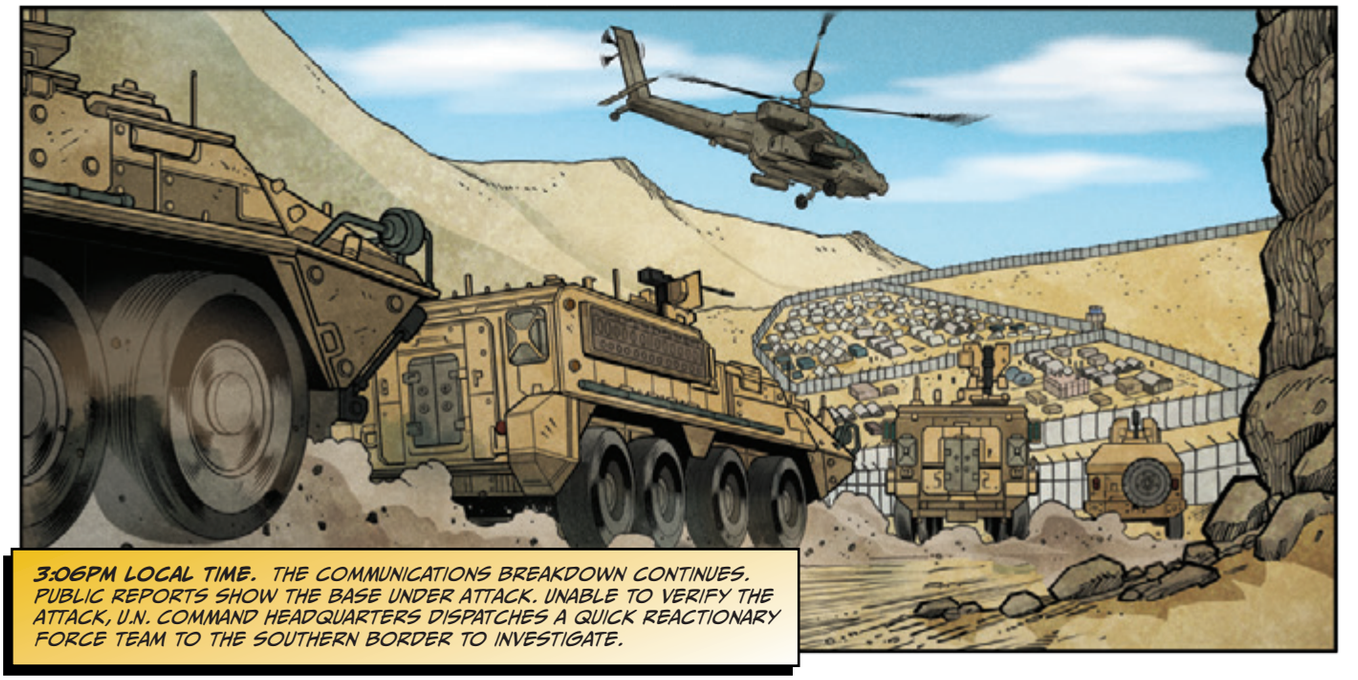

THE SECURE ACT WILL LIMIT EGREGIOUS DATA GATHERING AND HOW COMPANIES CAN PROFIT FROM THAT DATA.
IT WILL NOT LIMIT INNOVATION.
IT WILL PROTECT THE RIGHTS AND IDENTITIES OF AMERICAN CITIZENS!


BY SHAPING THE DEBATE IN CONGRESS, DONOVIA DISTRACTS LAW MAKERS AND THE MEDIA, POLARIZING AND SWAYING PUBLIC OPINION.

BACK IN ATROPIA... THE SITUATION ON THE GROUND CONTINUES TO DETERIORATE. WHILE THE LOCALS FOCUS ON CONVINCING THE AMERICANS THEIR VACCINES ARE POISON, DONOVIA MAKES ITS MOVE.

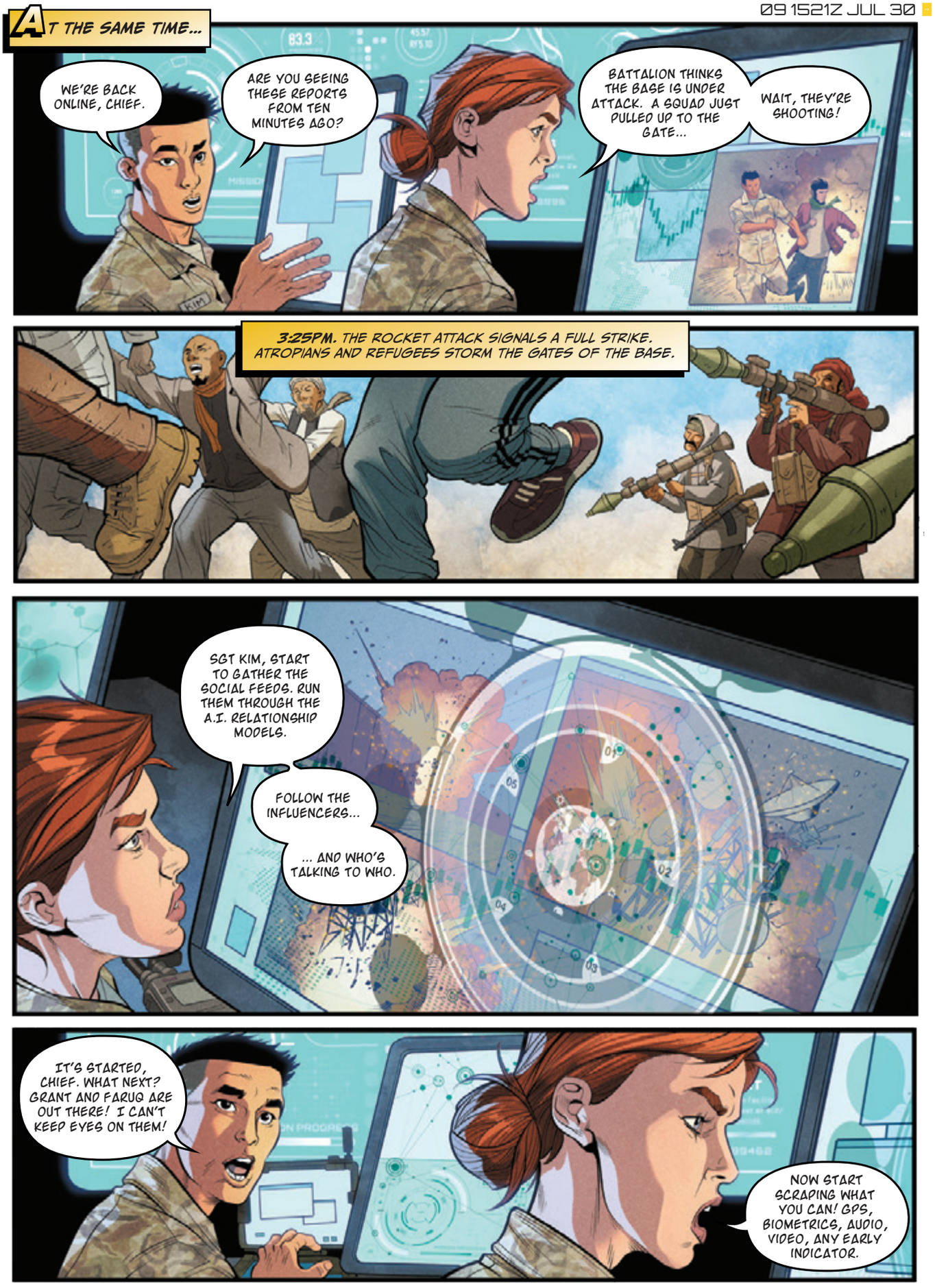


3:02PM LOCAL TIME. AN I.W. ATTACK INTERRUPTED THE BASE'S OUTGOING NETWORK. ONLY A SELECT FEW WITH MULTIPLE COMMUNICATION LINKS MADE IT THROUGH TO CONFIRM OR DENY THE ATTACK.



3:06PM LOCAL TIME. THE COMMUNICATIONS BREAKDOWN CONTINUES. PUBLIC REPORTS SHOW THE BASE UNDER ATTACK. UNABLE TO VERIFY THE ATTACK, U.N. COMMAND HEADQUARTERS DISPATCHES A QUICK REACTIONARY FORCE TEAM TO THE SOUTHERN BORDER TO INVESTIGATE.


AT 3:21PM THE QUICK REACTIONARY FORCE TEAM ARRIVES, SPARKING CHAOS.
BELIEVING THAT THE BASE IS UNDER ATTACK, THE ASSAULT TEAM TRIES TO SECURE THE AREA.
IN THE CRUSHING TENSION, VIOLENCE ERRUPTS.
DONOVIA UNLEASHES A BATTALION OF A.I. SOCIAL BOTS TO CAPTURE AND AMPLIFY THE SHOOTING.
THE REFUGEES RECEIVE UNCONFIRMED REPORTS THAT THE QUICK REACTIONARY FORCE IS COMING TO DRIVE THEM FROM THE CAMP.


AT THE SAME TIME...
WE'RE BACK ONLINE, CHIEF.
ARE YOU SEEING THESE REPORTS FROM TEN MINUTES AGO?
BATTALION THINKS THE BASE IS UNDER ATTACK. A SQUAD JUST PULLED UP TO THE GATE...
WAIT, THEY'RE SHOOTING!
3:25PM. THE ROCKET ATTACK SIGNALS A FULL STRIKE. ATROPIANS AND REFUGEES STORM THE GATES OF THE BASE.
SGT KIM, START TO GATHER THE SOCIAL FEEDS. RUN THEM THROUGH THE A.I. RELATIONSHIP MODELS.
FOLLOW THE INFLUENCERS...
... AND WHO'S TALKING TO WHO.
IT'S STARTED, CHIEF. WHAT NEXT? GRANT AND FARUQ ARE OUT THERE! I CAN'T KEEP EYES ON THEM!
NOW START SCRAPING WHAT YOU CAN! GPS, BIOMETRICS, AUDIO, VIDEO, ANY EARLY INDICATOR.


09 1527Z JUL 30
HEAVILY ARMED SEPARATISTS USE THE OPPORTUNITY TO PUSH THROUGH THE GATE. A FIRE FIGHT BREAKS OUT.
IN THE FIGHT, SGT GRANT IS CAPTURED AND TAKEN BY THE SEPARATISTS.
HE'S GONE! THEY TOOK HIM! THEY GOT SGT GRANT!

DRIP·FEED

I HAVE HIM HERE LADIES AND GENTS... SENATOR JIM RUSS! HERE TO TALK ABOUT HOW HIS MASTERPIECE IS ABOUT TO MAKE ITS WAY THROUGH THE GAUNTLET OF THE U.S. CONGRESS.

THE SECURE ACT. HAVE YA SEEN IT?

SENATOR JIM RUSS

THERE'S SOMETHING IN HERE FOR EVERYONE. DATA PRIVACY, NON-TRANSPARENCY, BIOMETRICS, A.I. ANALYSIS, DATA PROFITEERING...

IT'S ALL A NO FLY ZONE! HANDS OFF, YOU CORPORATE OVERLORDS!

NEEDED STEPS OR MASSIVE OVERREACH?

DOF LIVE

PROTECT OUR PRIVACY!

EXCLUSIVE NEWS INTERNATIONAL

#

@OversightWatchdog

Just Oct

Historic failures to scrutinize Donovian government-owned telecoms licensed to operate in the US.

#DataPrivacy

UMMM THOUGHT BLOCK FOLKS... I'M JUST SEEING THIS COME IN. THERE'S BEEN AN ATTACK ON THE U.N. BASE IN ATROPIA!

CONFLICTING MESSAGES, BUT THERE ARE CASUALTIES...

THE GATE WAS BREACHED AND THERE'S CONFIRMATION OF AT LEAST FOUR DEAD.

SEND ME WHAT YOU HAVE! I WANT EXCLUSIVE FOOTAGE!

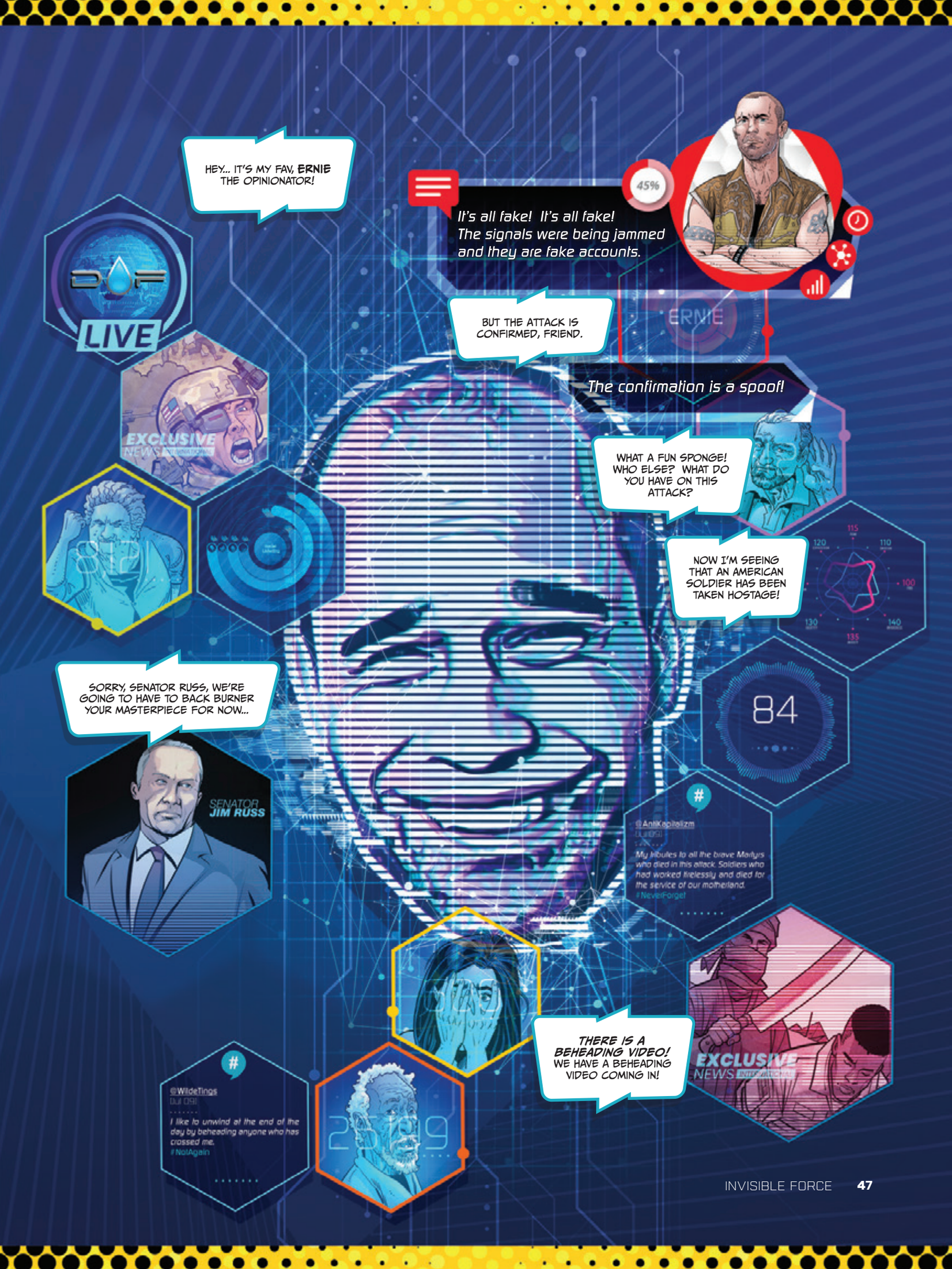
INCOMING NEWS INTERNATIONAL

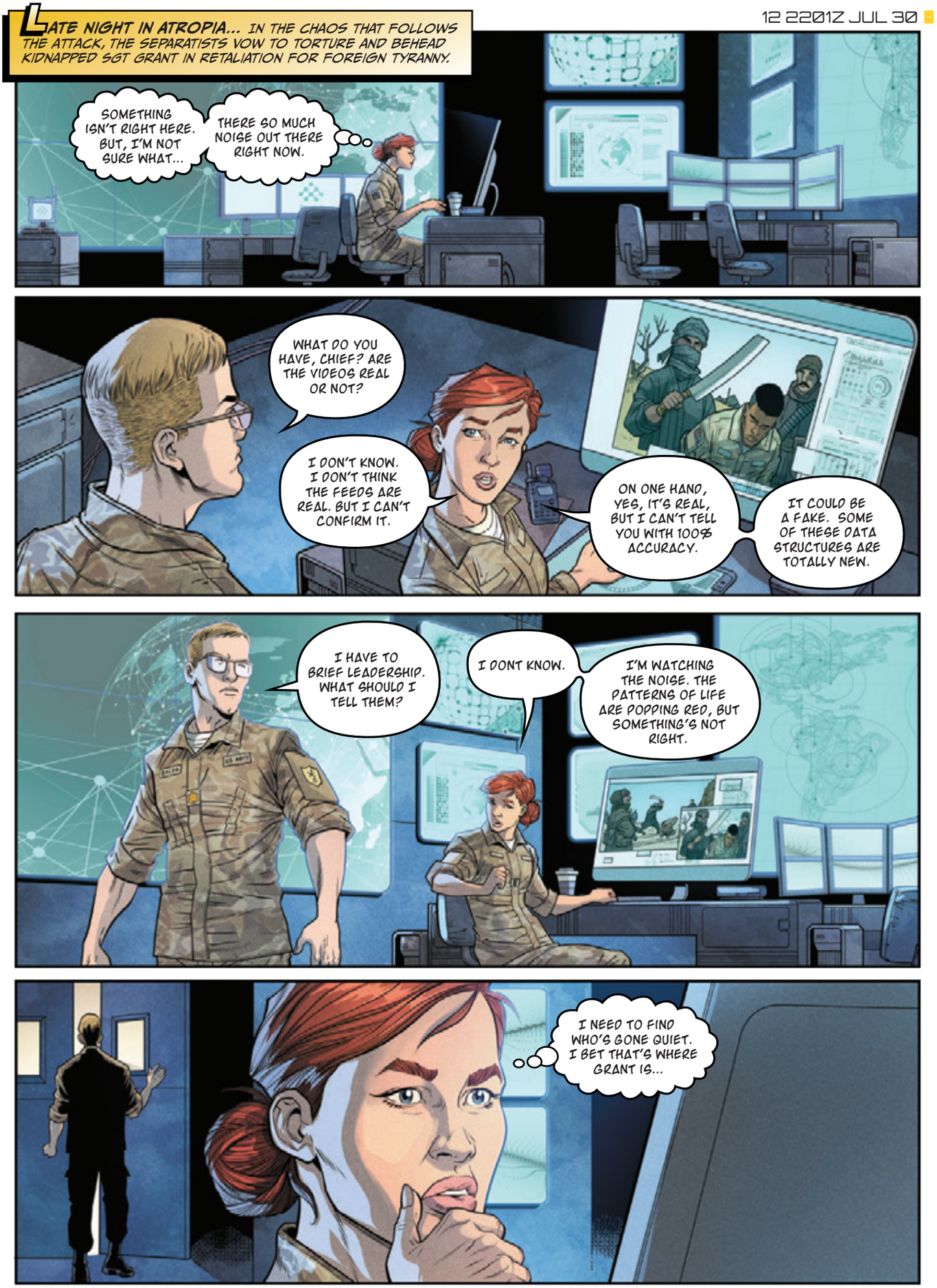
EXCLUSIVE NEWS INTERNATIONAL

#

@SeeNoMore

Just Oct


HEY... IT'S MY FAV, ERNIE THE OPINIONATOR!
45%
It's all fake! It's all fake! The signals were being jammed and they are fake accounts.
ERNIE
BUT THE ATTACK IS CONFIRMED, FRIEND.
The confirmation is a spoof!
WHAT A FUN SPONGE! WHO ELSE? WHAT DO YOU HAVE ON THIS ATTACK?
NOW I'M SEEING THAT AN AMERICAN SOLDIER HAS BEEN TAKEN HOSTAGE!
SORRY, SENATOR RUSS, WE'RE GOING TO HAVE TO BACK BURNER YOUR MASTERPIECE FOR NOW...
SENATOR JIM RUSS
84
@AntiKapitalizm
My tributes to all the brave Martyrs who died in this attack. Soldiers who had worked tirelessly and died for the service of our motherland.
#NeverForget
THERE IS A BEHEADING VIDEO! WE HAVE A BEHEADING VIDEO COMING IN!
EXCLUSIVE NEWS
@WildeTings
I like to unwind at the end of the day by beheading anyone who has crossed me.
#NotAgain
LIVE
EXCLUSIVE NEWS


LATE NIGHT IN ATROPIA... IN THE CHAOS THAT FOLLOWS THE ATTACK, THE SEPARATISTS VOW TO TORTURE AND BEHEAD KIDNAPPED SGT GRANT IN RETALIATION FOR FOREIGN TYRANNY.
SOMETHING ISN'T RIGHT HERE. BUT, I'M NOT SURE WHAT...
THERE SO MUCH NOISE OUT THERE RIGHT NOW.
WHAT DO YOU HAVE, CHIEF? ARE THE VIDEOS REAL OR NOT?
I DON'T KNOW. I DON'T THINK THE FEEDS ARE REAL. BUT I CAN'T CONFIRM IT.
ON ONE HAND, YES, IT'S REAL, BUT I CAN'T TELL YOU WITH 100% ACCURACY.
IT COULD BE A FAKE. SOME OF THESE DATA STRUCTURES ARE TOTALLY NEW.
I HAVE TO BRIEF LEADERSHIP. WHAT SHOULD I TELL THEM?
I DONT KNOW.
I'M WATCHING THE NOISE. THE PATTERNS OF LIFE ARE POPPING RED, BUT SOMETHING'S NOT RIGHT.
I NEED TO FIND WHO'S GONE QUIET. I BET THAT'S WHERE GRANT IS...

01

Shoshana Zuboff

The Age of Surveillance Capitalism
(PublicAffairs, 2019)

QUOTE FROM: "THE AGE OF SURVEILLANCE CAPITALISM"

"The future cyber domain will no longer be defined by clear boundaries between online and offline. The explosion of computer power and the integration of computers into everyday life has come with some significant, and largely unexamined, opportunities but also consequences. Leaders in all domains need to be aware of the ubiquity of technology and the impact that it has on the world around it. Put another way, technology is no longer a passive member of our world – through algorithms, technology is rapidly changing the way that humans interact with their environment and with each other[1]."

ACROSS THE BASE...

02

QUOTE FROM: "DISINFORMATION AS COLLABORATIVE WORK"

Kate Starbird

"Disinformation as Collaborative Work: Surfacing the Participatory Nature of Strategic Information Operations"
CSCW, (2019)

"Strategic information operations are a global phenomenon, with political, social, psychological, educational, and cybersecurity dimensions. Strategic information operations, and in particular disinformation, function to undermine the integrity of the information space and reduce human agency by overwhelming our capacity to make sense of information [66, 69]. They therefore strike at the core of our values. And they affect things we care about—for example, finding life-saving information during a crisis event [85, 95], organizing online for political change [87, 96, 104], and protecting online spaces from bullying and harassment. [10, 97][2]"

IN THE NEARBY TOWN...

03

QUOTE FROM: "MINDF*CK"

Christopher Wylie

*Mindf*ck: Cambridge Analytica and the Plot to Break America*
(New York: Random House, 2019)

"The rights to life, liberty, association, speech, vote, and conscience are all underpinned with a presumption of agency, as they are outputs of that agency...We cannot be free to choose if our choices are monitored and filtered for us...Privacy is the very essence of our power to decide who and how we want to be. Privacy is not about hiding—privacy is about human growth and agency. But this is not merely about privacy or consent. This is about who gets to influence our truths and the truths of those around us. This is about the architectures of manipulation we are constructing around our society.[3]"

AROUND THE WORLD...

04

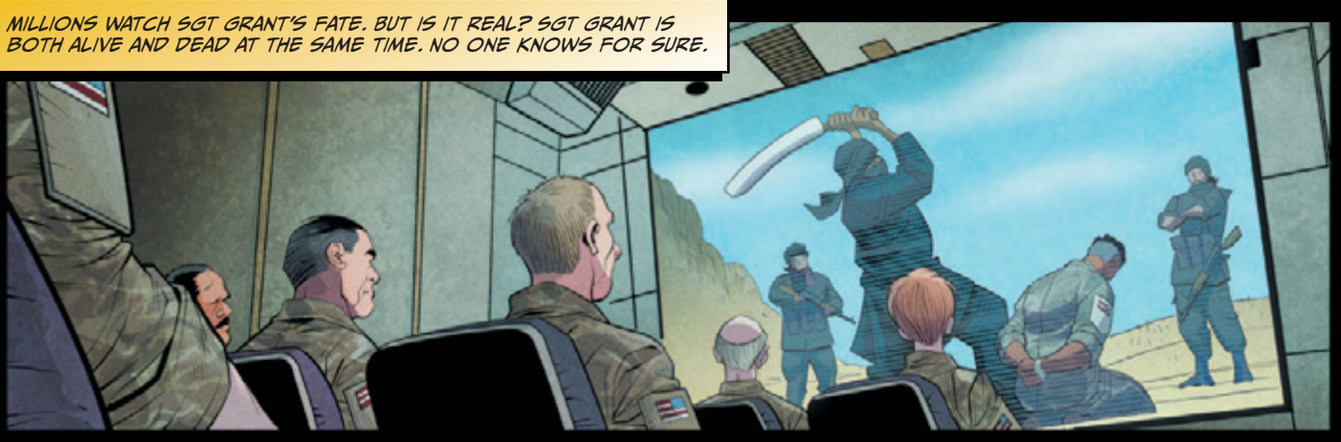
QUOTE FROM: "VIEW OF ENGINEERING THE PUBLIC"

Zeynep Tufekci

"*View of Engineering the Public: Big Data, Surveillance and Computational Politics*", ***First Monday,*** (2014)

"Digital technologies have given rise to a new combination of big data and computational practices which allow for massive, latent data collection and sophisticated computational modeling, increasing the capacity of those with resources and access to use these tools to carry out highly effective, opaque and unaccountable campaigns of persuasion and social engineering in political, civic and commercial spheres. What are the consequences of these new mechanisms on the public sphere and political campaigns?[4]"

MILLIONS WATCH SGT GRANT'S FATE. BUT IS IT REAL? SGT GRANT IS BOTH ALIVE AND DEAD AT THE SAME TIME. NO ONE KNOWS FOR SURE.



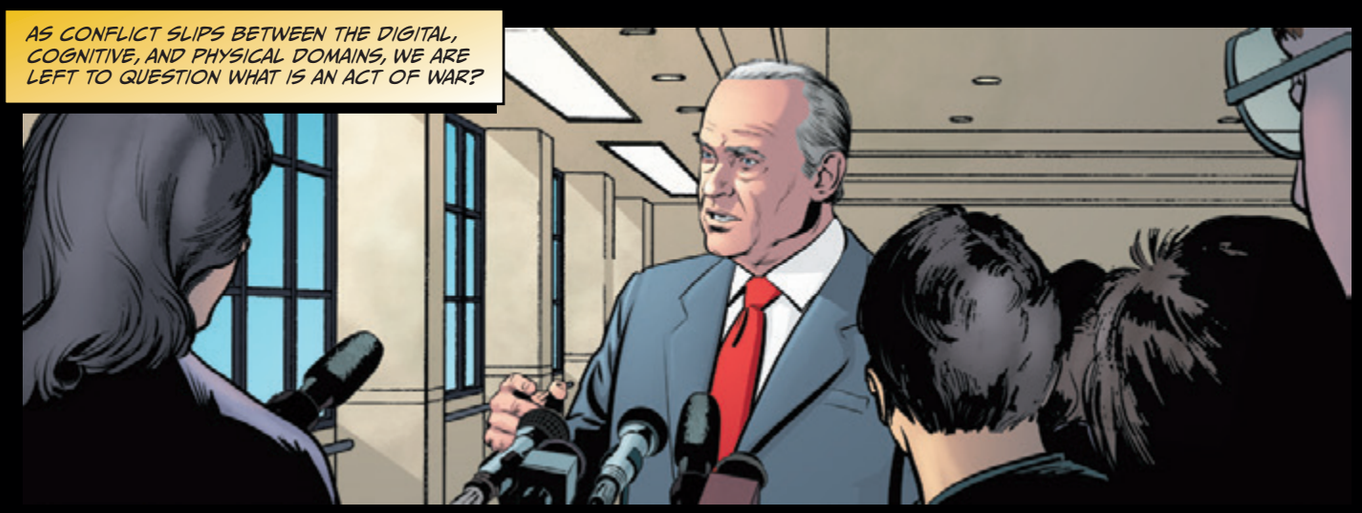
05

THE FUTURE OF CONFLICT

Jessica I. Dawson Ph.D.,
Major
Assistant Professor
Army Cyber Institute

Robert Ross, Ph.D.
Lieutenant Colonel
Chief Research Scientist
Army Cyber Institute

"The practiced, age-old art of deception is currently being leveraged in novel ways that will become increasingly more sophisticated in the future. Deep-fake content is the technical manipulation of digital video, audio, picture, and text data in ways that appear authentic. These technologies use deep learning technologies to create technologically produced disinformation. Powerful attacks, such as these, manipulate a targeted audience's beliefs and how they determine truth. They are designed to create division, confusion, and uncertainty and multiple states of truth. The use of deep-fake content driven disinformation attacks produce radical political and social reactions when directed at diverse populations in proximity of one another. What are the consequences of the algorithm-enhanced proliferation of deep-fake content within local communities the U.S. military is operating among while deployed abroad?"



06

QUOTE FROM: "MINDF*CK"

Christopher Wylie

*Mindf*ck: Cambridge Analytica and the Plot to Break America*
(New York: Random House, 2019)

"The rights to life, liberty, association, speech, vote, and conscience are all underpinned with a presumption of agency, as they are outputs of that agency. But agency itself has not been articulated as a right per se, as it has always been presumed to exist simply by virtue of our personhood….Privacy is the very essence of our power to decide who and how we want to be. Privacy is not about hiding—privacy is about human growth and agency."

07

QUOTE FROM: "UNMASKING MASKIROVKA"

Daniel Bagge

Unmasking Maskirovka: Russia's Cyber Influence Operations
(Defense Press, 2019)

"Influence campaigns surround us every day, whether with malicious intent or for product and service advertisement. Asking whether influence operations are on the rise is irrelevant. The more pertinent question is instead whether one is susceptible to them and, if so, how they work so one can understand them and become resilient against any adverse effects they might present….The conduct of influence campaigns is usually part of a broader set of activities, such as those visible in so-called grey-zone conflicts in recent years.[5]"

08 QUOTE FROM: "UNMASKING MASKIROVKA"

"A fundamental way to understand influence campaigns is by categorizing their events and influence activities and then, where possible, correlating the findings with known patterns from the last century.…Influence activities include: …state control over media, subjugation of political parties, fraudulent elections, using blogs and trolls and social networks for information operations, pacification of intellectual opponents, such as non-governmental organizations, attacks against proclaimed enemies of the state - political opponents domestically and internationally, creation of pro-government mass media engaged in disinformation campaigns, dissemination of disinformation to undermine conventional press, gaining political influence in foreign countries, production of pro-government non-governmental organizational advancing the foreign policy goals favored by the establishment.[6]"

Daniel Bagge

Unmasking Maskirovka: Russia's Cyber Influence Operations
(Defense Press, 2019)

09 QUOTE FROM: "UNMASKING MASKIROVKA"

"Deception 101 - Primer on Deception, the U.S. view of strategic, operational and tactical deceptions are:[11] Strategic deception intends to "disguise basic objectives, intentions, strategies, and capabilities." Operational deception, which confuses an adversary regarding "a specific operation or action you are preparing to conduct." Tactical deception is intended to mislead "others while they are actively involved in competition with you, your interests, or your forces.[7]"

Daniel Bagge

Unmasking Maskirovka: Russia's Cyber Influence Operations
(Defense Press, 2019)

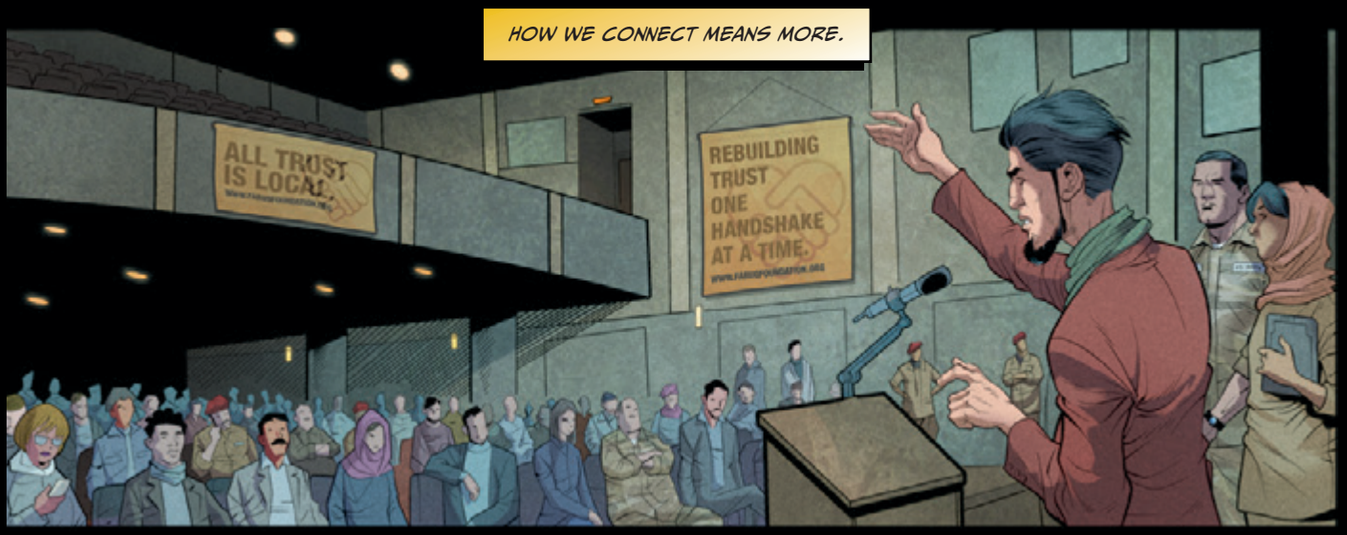
10

QUOTE FROM: "SANDWORM"

Andy Greenberg

Sandworm: A New Era of Cyberwar and the Hunt for the Kremlin's Most Dangerous Hackers (Doubleday, 2019)

"We're seeing more aggressive, numerous actions than I've seen in ten-plus years of doing this. A primary reason for that escalation is...The U.S. government, and the West as a whole, have failed to set the norms that might keep the march toward cyberwar in check…. Every country's intelligence agencies that witness another country's hacking capabilities… immediately seek to match or overtake their foes. The powers of disruption…weren't an aberration. They're merely the most visible model of a tool kit that every militarized nation and rogue state in the world might soon covet or possess: the new standard arsenal for a global cyberwar standoff.[8]"



11	QUOTE FROM: "SKIN IN THE GAME"
Nassim Nicholas Taleb *Skin in the Game: Hidden Asymmetries in Daily Life* (Random House, 2017)	"Groups behave differently at a different scale. This explains why the municipal is different from the national. It also explains how tribes operate: you are part of a specific group that is larger than the narrow you, but narrower than humanity in general….There is no way you can get the same cohesion in a larger city when the "other" is a theoretical entity, and our behavior toward him or her is governed by some general ethical rule, not someone in flesh and blood. We get it easily when seen that way, but fail to generalize that ethics is something fundamentally local. Now what's the reason? Modernity put it in our heads that there are two units: the individual and the universal collective—in that sense, skin in the game for you would be just for you, as a unit. In reality, my skin lies in a broader set of people, one that includes a family, a community, a tribe, a fraternity. But it cannot possibly be the universal.[9]"

12	QUOTE FROM: "A RUBICON"
Daniel Geer *"A Rubicon"* ***Aegis Series Paper No. 1801*** (2018)	"Consent of the governed is democracy's core requirement and democracy's core deliverable alike. Consent of the governed begins with the common acceptance that man's rule of men is accountable to an authority higher than man….Undemocratic regimes do not indulge in niceties like "consent of the governed," and as the Wall Street Journal has already observed, "Information technology, far from undermining China's authoritarian model as many thought it would, is reinforcing it.[10]"

13

Shoshana Zuboff

The Age of Surveillance Capitalism
(PublicAffairs, 2019)

QUOTE FROM: "THE AGE OF SURVEILLANCE CAPITALISM"

"[Surveillance capitalism] revealed new capabilities to infer and deduce the thoughts, feelings, intentions, and interests of individuals and groups with an automated architecture that operates as a one-way mirror irrespective of a person's awareness, knowledge, and consent, thus enabling privileged secret access to behavioral data. A one-way mirror embodies the specific social relations of surveillance based on asymmetries of knowledge and power.[11]"

14

Daniel Bagge

Unmasking Maskirovka: Russia's Cyber Influence Operations
(Defense Press, 2019)

QUOTE FROM: "UNMASKING MASKIROVKA"

"Deception maintains a long tradition as a tool in military and political conflict. It does not remain unique to the activities of humanity, as examples of camouflage, concealment, and misleading features and behavior are common in nature. Deceptive conduct, camouflage, protective elements of coloration, shape, and masking are present in the realm of fauna and flora. The effectiveness of deception is unquestionable.[12]"

15

Shoshana Zuboff

The Age of Surveillance Capitalism
(PublicAffairs, 2019)

QUOTE FROM: "THE AGE OF SURVEILLANCE CAPITALISM"

"[Privacy] policies had to enforce secrecy in order to protect operations that were designed to be undetectable because they took things from users without asking and employed those unilaterally claimed resources to work in the service of others' purposes... This power is a crucial illustration of the difference between "decision rights" and "privacy." Decision rights confer the power to choose whether to keep something secret or to share it. One can choose the degree of privacy or transparency for each situation. U.S. Supreme Court Justice William O. Douglas articulated this view of privacy in 1967: "Privacy involves the choice of the individual to disclose or to reveal what he believes, what he thinks, what he possesses...." Surveillance capitalism lays claim to these decision rights. The typical complaint is that privacy is eroded, but that is misleading. In the larger societal pattern, privacy is not eroded but redistributed, as decision rights over privacy are claimed for surveillance capital. Instead of people having the rights to decide how and what they will disclose, these rights are concentrated within the domain of surveillance capitalism.[13]"


OR IS THERE STILL HOPE?
BAKER
U.S
I FOUND THE SILENCE IN THE NOISE. I FOUND HIM! SGT GRANT IS ALIVE!
WE GOT HIM. WE GOT SGT GRANT. HE'S BANGED UP BUT HE'S ALIVE.
END.

Excerpt from **"A RUBICON"**

"Interdependence within society today is centered on the Internet beyond all other dependencies excepting climate, and the Internet has a time constant of change five orders of magnitude smaller than that of climate. Our concern is unacknowledged correlated risk, the unacknowledged correlated risk of cyberspace is why cyberspace is capable of black swan behavior. So, if our "critical infrastructures are those physical and cyber–based systems essential to the minimum operations of the economy and government", and if aggregate risk is growing steadily (as leading cybersecurity operational managers confirm), then do we put more of our collective power behind forcing security improvements that can only be increasingly diseconomic, or do we preserve fallbacks of various sorts in anticipation of events more likely to happen as time passes?

Conservative prudence says that retaining human skills, like retaining human languages, will not be justified by any balance sheet, only by societal wisdom in the large. Conservative risk management says that if you don't know how "it" works then you won't manage its risks. Or, as they say in the poker world, if after ten minutes at the table you don't know who the patsy is—you're the patsy.

The essence of security in places of public assembly is the provision of sufficient, tested exits through which the audience can leave in short enough order that all they lose is the remainder of the play. As a matter of national security, keeping non–technical exits open requires action and it requires it now. It will not happen by itself, and it will never again be as cheap or feasible as it is now. Never again will national security and individual freedom jointly share a call for the same initiative at the same time.

We will never have a more analog world than we have now. We will never live under thinner–tailed distributions than we have now, at least so long as we demand freedom. Countries that built complete analog physical plants have a signal advantage over countries that leapfrogged directly to full digitalization. The former countries have preservable and protective firebreaks in place that the latter will never have, but the former countries enjoy their resilience dividend if, and only if, they preserve their physical plant. That such preservation can deliver both resilience for the digitalized and continued freedom for those choosing not to participate in digitalization is unique to this historical moment. We stand on the bank of our Rubicon.[14]"

– Daniel E. Geer
Hoover Institute

AFTERWORD

This story was designed to help the military and leaders from all walks of life conceptualize what the future of information warfare might look like. Fundamentally, with the interconnected nature of daily life, information warfare is something that is no longer limited to the traditional domains of war. America's adversaries have realized that we are unbeatable on the traditional battlefield not only due to our military capabilities, but for our uncanny ability to come together to solve collective problems. As a result, our adversaries are switching tactics, utilizing old tactics in new domains – deception, disinformation, and misinformation are just a few of these techniques being digitized and weaponized – all to erode trust.

The fundamental assumption about connecting things on the Internet involved misplaced trust – trust that people in society are basically good. Trust is fundamental in open societies. But trust in institutions has been eroding over the last few generations and the increasing geographic, educational, and political segregation has further eroded trust. Social media, combined with disinformation campaigns, has merely been an accelerant on a preexisting condition.

The central problem facing societies impacted by automated disinformation strikes is the heart of the collective action problem. Cognitive segregation will continue to erode and undermine societies' ability to act as a collective unit – the nation that figures out how to solve this post–truth problem will be able to effectively defend against the future of information war. We will be unable to muster the ability to go to war if we cannot agree on who the enemy is.

ObiWan Kenobi famously told Luke Skywalker that he'd told him the truth about his father – from a certain point of view. There are some things that are fundamentally true whether people agree on them or not. Fear is one of those fundamental truths about human society: when people are afraid, they will react with "almost mathematically certainty" against the thing they fear[1]. As long as disinformation strikes at things people are afraid of, our adversaries will be able to exploit the thing that is America's greatest strength.

[1] William L. Shirer and Ron Rosenbaum, The Rise and Fall of the Third Reich, Reissue edition (RosettaBooks, 2011).

Other truths are a matter of perspective, but trust and truth go hand in hand. Rebuilding fractured trust requires the truth – and the algorithms influencing everyday lives fundamentally obscure the truth. Who do we hold accountable if the algorithm decides to tell your self–driving car to drive off a cliff? More realistically, who do we hold accountable if an algorithm floods news feeds with fake news that is purely automated content?

The "Invisible Force" in this story was an adversarial nation state, but Drip•Feed was merely an algorithm doing what it was designed to do – stir up controversial news opinions and generate Internet traffic. Both invisibly attacked the foundational structures of another society. By monitoring social media, the Donovians were able to fire an American employee who said something against Donovia – but don't Americans have the right to free speech?

The "Invisible Force" attacked the military's ability to make decisions – the ability to make assumptions is a key aspect of military decision making process and yet, they could not assume whether SGT Grant was alive or dead – they genuinely had no idea and the courses of action developed differed drastically based on their interpretations of the truth. They could believe he was alive or dead at the same time but, fundamentally, only one of those things was actually true. It was not a matter of perspective.

The future of information war is the future of military conflict. With any luck, this book helps leaders visualize the complexity of that fight – and starts to generate a conversation around planning to overcome the next "Invisible Force".

– Major Jessica I. Dawson Ph.D.
Assistant Professor
Army Cyber Institute

ENDNOTES

Microtargeting as Information War (p.16-17):

[1] DARPA, "Narrative Networks," **Defense Advanced Research Projects Agency** (2011), https://www.darpa.mil/program/narrative-networks.

[2] "Joint Publication 3-13.2: Military Information Support Operations", **Department of Defense, December 20, 2011**, https://www.bits.de/NRANEU/others/jp-doctrine/JP3-13.2C1(11).pdf.

[3] S. C. Matz et al., "Psychological Targeting as an Effective Approach to Digital Mass Persuasion," **Proceedings of the National Academy of Sciences** 114, no. 48 (November 28, 2017): 12714, https://doi.org/10.1073/pnas.1710966114.

[4] Sasha Issenberg, **The Victory Lab: The Secret Science of Winning Campaigns**, Reprint Edition (New York: Broadway Books, 2013).

[5] Christopher Wylie, **Mindf*ck: Cambridge Analytica and the Plot to Break America** (New York: Random House, 2019).

[6] Shoshana Zuboff, **The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power,** 1 edition (PublicAffairs, 2019).

[7] Michael Schudson, **Advertising, The Uneasy Persuasion: Its Dubious Impact On American Society,** Reprint edition (New York: Basic Books, 1986).

[8] Wylie, **Mindf*ck**; Brittany Kaiser, **Targeted: The Cambridge Analytica Whistleblower's Inside Story of How Big Data, Trump, and Facebook Broke Democracy and How It Can Happen Again** (Harper, 2019); Issenberg, The Victory Lab.

[9] Zeynep Tufekci, **Twitter and Tear Gas: The Power and Fragility of Networked Protest,** Reprint edition (New Haven London: Yale University Press, 2018).

[10] Brittany Kaiser, **Targeted: The Cambridge Analytica Whistleblower's Inside Story of How Big Data, Trump, and Facebook Broke Democracy and How It Can Happen Again** (Harper, 2019); Issenberg, The Victory Lab, 384.

[11] Christopher Wylie, **Mindf*ck: Cambridge Analytica and the Plot to Break America** (New York: Random House, 2019), 49.

[12] Stuart A Thompson and Charlie Warzel, "Twelve Million Phones, One Dataset, Zero Privacy," **New York Times,** December 19, 2019, Online Edition edition.

[13] Christopher Wylie, **Mindf*ck: Cambridge Analytica and the Plot to Break America** (New York: Random House, 2019), 67.

[14] Matz et al., "Psychological Targeting as an Effective Approach to Digital Mass Persuasion," 12714.

[15] Zeynep Tufekci, "View of Engineering the Public: Big Data, Surveillance and Computational Politics | First Monday," **First Monday** 19, no. 7 (2014): 1, https://firstmonday.org/ojs/index.php/fm/article/view/4901/4097.

[16] Adam Zewe, "Imperiled Information: Students Find Website Data Leaks Pose Greater Risk than Most People Realize," Harvard John A. Paulson School of Engineering and Applied Sciences, January 17, (2020), https://www.seas.harvard.edu/news/2020/01/imperiled-information.

[17] 116th Congress, "REPORT OF THE SELECT COMMITTEE ON INTELLIGENCE UNITED STATES SENATE ON RUSSIAN ACTIVE MEASURES CAMPAIGNS AND INTERFERENCE IN THE 2016 U.S.ELECTION," Senate Report (Washington, D.C.: United States Senate Intelligence Committee, 2017), https://www.intelligence.senate.gov/sites/default/files/documents/Report_Volume1.pdf.

[18] Claire Allbright, "A Russian Facebook Page Organized a Protest in Texas. A Different Russian Page Launched the Counterprotest.," **The Texas Tribune,** November 1, 2017, https://www.texastribune.org/2017/11/01/russian-facebook-page-organized-protest-texas-different-russian-page-l/; Andrew Weisburd, Clint Watts, and Jm Berger, "Trolling for Trump: How Russia Is Trying to Destroy Our Democracy," **War on the Rocks,** November 6, 2016; Ryan Browne, "Russian Trolls Tried to Convince African Americans Not to Vote in 2016, US Senate Says," CNBC, October 9, 2019, https://www.cnbc.com/2019/10/09/senate-intel-report-russian-trolls-targeted-african-americans-in-2016.html.

[19] Rachelle Hampton, "Years Ago, Black Feminists Worked Together to Unmask Twitter Trolls Posing as Women of Color. If Only More People Paid Attention.," **Slate Magazine,** April 23, 2019, https://slate.com/technology/2019/04/black-feminists-alt-right-twitter-gamergate.html.

[20] Ralph K. White, "Propaganda: Morally Questionable and Morally Unquestionable Techniques," **The ANNALS of the American Academy of Political and Social Science** 398, no. 1 (November 1971): 26–35, https://doi.org/10.1177/000271627139800104.

ENDNOTES

[21] Sandeep Suntwal, Susan A Brown, and Mark W Patton, "How Does Information Spread? A Study of True and Fake News," n.d., 10.

[22] Francesca Polletta and Jessica Callahan, "Deep Stories, Nostalgia Narratives, and Fake News: Storytelling in the Trump Era," **American Journal of Cultural Sociology** 5, no. 3 (October 2017): 392–408, https://doi.org/10.1057/s41290-017-0037-7.

[23] Joseph E. Stiglitz, **The Price of Inequality: How Today's Divided Society Endangers Our Future,** 1 edition (New York: W. W. Norton & Company, 2012).

[24] Renee DiResta, "Computational Propaganda: If You Make It Trend, You Make It True," **The Yale Review,** October 9, 2018, https://yalereview.yale.edu/computational-propaganda.

The Future of Conflict (p.49-59):

[1] Shoshana Zuboff, **The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power**, 1 edition (PublicAffairs, 2019).

[2] Kate Starbird, Ahmer Arif, and Tom Wilson, "Disinformation as Collaborative Work: Surfacing the Participatory Nature of Strategic Information Operations," **Proceedings of the ACM on Human-Computer Interaction** 3, no. CSCW (November 7, 2019): 1–26, https://doi.org/10.1145/3359229.

[3] Christopher Wylie, **Mindf*ck: Cambridge Analytica and the Plot to Break America** (New York: Random House, 2019), 28.

[4] Christopher Wylie, **Mindf*ck: Cambridge Analytica and the Plot to Break America** (New York: Random House, 2019), 28.

[5] Daniel Bagge, **Unmasking Maskirovka: Russia's Cyber Influence Operations** (Defense Press, 2019), 22.

[6] Daniel Bagge, **Unmasking Maskirovka: Russia's Cyber Influence Operations** (Defense Press, 2019), 22.

[7] Daniel Bagge, **Unmasking Maskirovka: Russia's Cyber Influence Operations** (Defense Press, 2019), 29.

[8] Andy Greenberg, **Sandworm: A New Era of Cyberwar and the Hunt for the Kremlin's Most Dangerous Hackers** (Doubleday, 2019), 392.

[9] Nassim Nicholas Taleb, **Ski in in the Game: Hidden Asymmetries in Daily Life** (New York: Random House, 2018), 106.

[10] Daniel Geer, "A Rubicon," **Aegis Paper Series** (Stanford University: Hoover Institute, February 2018), https://www.hoover.org/sites/default/files/research/docs/geer_webreadypdfupdated2.pdf.

[11] Shoshana Zuboff, **The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power**, 1 edition (PublicAffairs, 2019).

[12] Daniel Bagge, **Unmasking Maskirovka: Russia's Cyber Influence Operations** (Defense Press, 2019), 28.

[13] Shoshana Zuboff, **The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power**, 1 edition (PublicAffairs, 2019).

[14] Daniel Geer, "A Rubicon," **Aegis Paper Series** (Stanford University: Hoover Institute, February 2018), https://www.hoover.org/sites/default/files/research/docs/geer_webreadypdfupdated2.pdf.

CREATIVE INDEX

Executive Producer: Shyama Helin

Creative Director: Sandy Winkelman

Writer: Brian David Johnson

Production Coordinator: Steve Buccellato

Special Advisors: MAJ Jessica I. Dawson, Ph.D.
LTC Robert Ross, Ph.D.

Main Drama:
Artist: Paco Diaz
Inker: Keith Champagne
Colorist: Rex Lokus

Interstitial Drama #1:
Artist: John McCrea
Inker: John McCrea
Colorist: Patricia Mulvihill

Drip Feed:
Artist: Steve Buccellato
Inker: Steve Buccellato
Colorist: Steve Buccellato
Graphic Design: Sandy Winkelman

Interstitial Drama #2:
Artist: Giuseppi Cafaro
Inker: Giuseppi Cafaro
Colorist: Guy Major

Interstitial Drama #3:
Artist: Matt Haley
Inker: Matt Haley
Colorist: Guy Major

ACKNOWLEDGMENTS

Thank you to all the experts and contributors who provided the team with invaluable ideas, insights, and technical knowledge.

LTC Robert Ross, Ph.D.
MAJ Jessica I. Dawson, Ph.D.
COL Andrew Hall Ph.D.
Peter W. Singer
August Cole
Renny Gleeson
Bruce Schnieier
Lee McIntyre, Ph.D.
MAJ Steve Whitham
MAJ Roy Ragsdale
Dr. Ed Sobiesk
LTC Douglas Fletcher, Ph.D.
LTC Erica Mitchell, Ph.D.
Celeste Evans
MAJ Lisa Beum
Courtney Gordon-Tennant
Sarah Cox-Gardner
LTC Natalie Vanatta
Cyndi Coon
Arizona State University:
The School for the Future of Innovation in Society
The Center for Science and the Imagination
The Applied Research Lab (ASURE)
The Threatcasting Lab

Printed in the United States of America
First Edition, 2020

http://cyber.army.mil

Threatcasting Lab
at Arizona State University
http://threatcasting.com

Arizona State University
http://www.asu.edu

Army Cyber Institute at West Point
http://cyber.army.mil