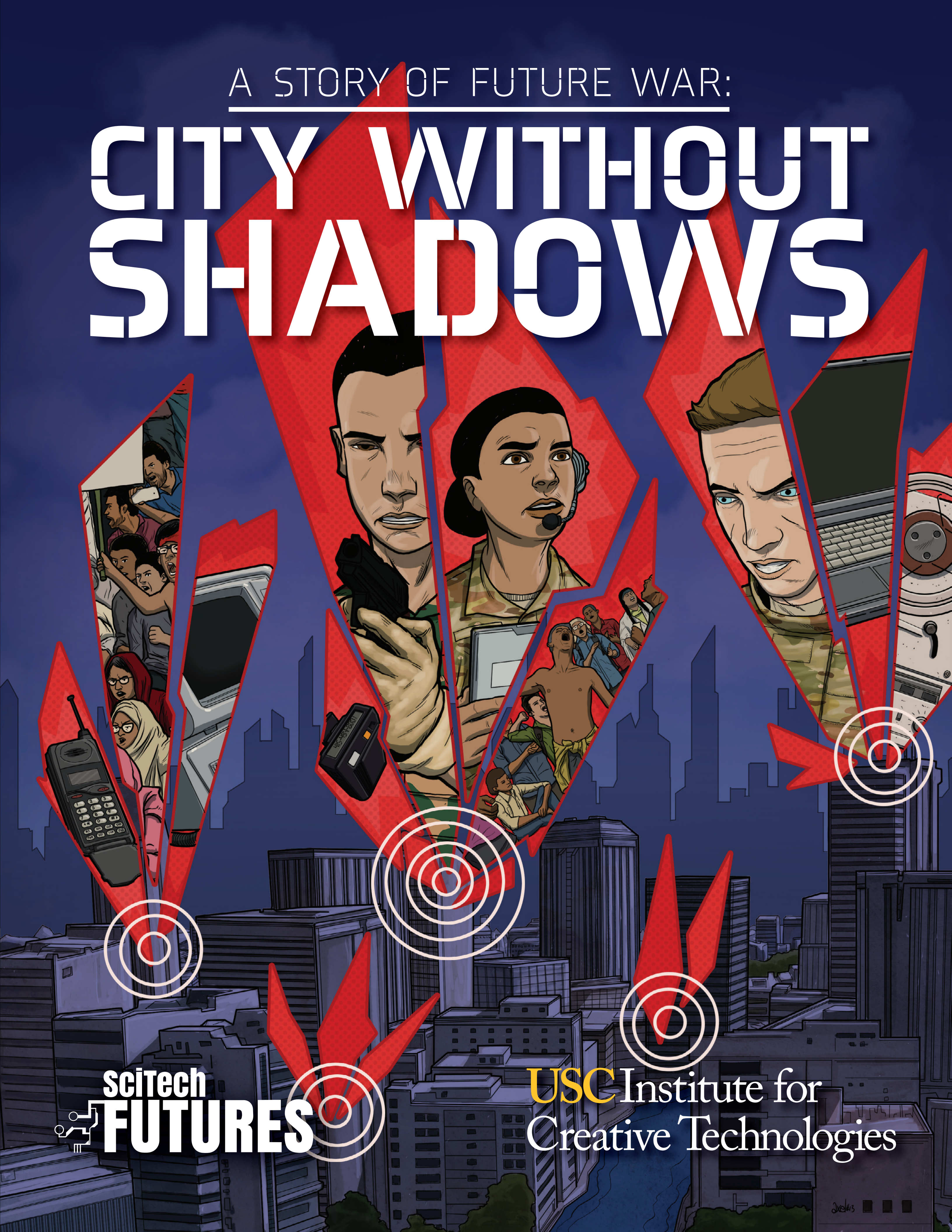
A STORY OF FUTURE WAR:

CITY WITHOUT SHADOWS



SciTech FUTURES

USC Institute for Creative Technologies

A STORY OF FUTURE WAR:

CITY WITHOUT SHADOWS

The story and its near future tech concepts are a result of the SciTech Futures Technology Foresight Exercise: Sustainment, Logistics, and the Urban Environment of 2035. The exercise began with an online ideation workshop conducted by the University of Southern California's Institute for Creative Technologies.

Following the online workshop, USC ICT and FutureScout LLC conducted an in-person exercise. 15 participants were invited to explore the results of the online workshop and use them as source material for a guided ideation session. Participants were recruited from a variety of backgrounds, including film and television screenwriters and consultants, retired and active duty Soldiers and Marines, a USMA cadet, and academic and industry GEOINT experts.

You can read more about the major near future tech concepts introduced in the pages following the story.

Find out more about these exercises at https://futures.armyscitech.com/

written by Anthony DeCapite

art by Axel Ortiz

colors by Daniel Toledo

edited by Asa Shumskas Tait

additional concept art by Michael Gizienski,
Scott Carter, Jon Smith

Special thanks to the online workshop users for their contributions, especially *creepyswampthing* for the City Without Shadows phrase and thematic concept, *jkadtke* for the Mirror City concept, *souhan* for the EW Minefield, and *nmk47* for the synthetic, microbial forensic tracer concept.

Supported by the SciTech Futures Technology Effort under the office of the Deputy Assistant Secretary of the Army (Research & Technology). The views and opinions of authors expressed herein do not necessarily state or reflect official views or policies of the United States Army.

DHAKA, BANGLADESH - 2035

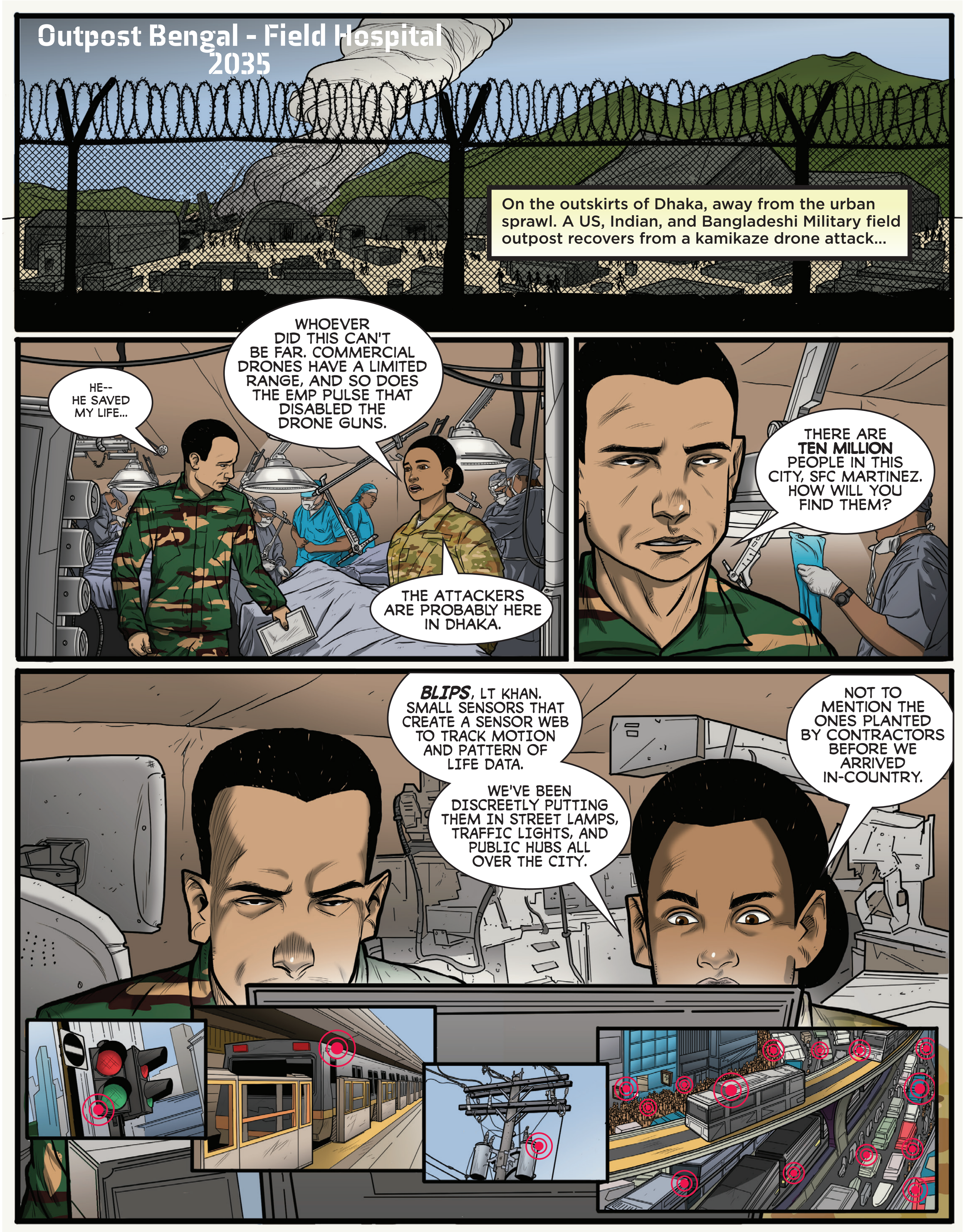
Bangladesh is at a crossroads.

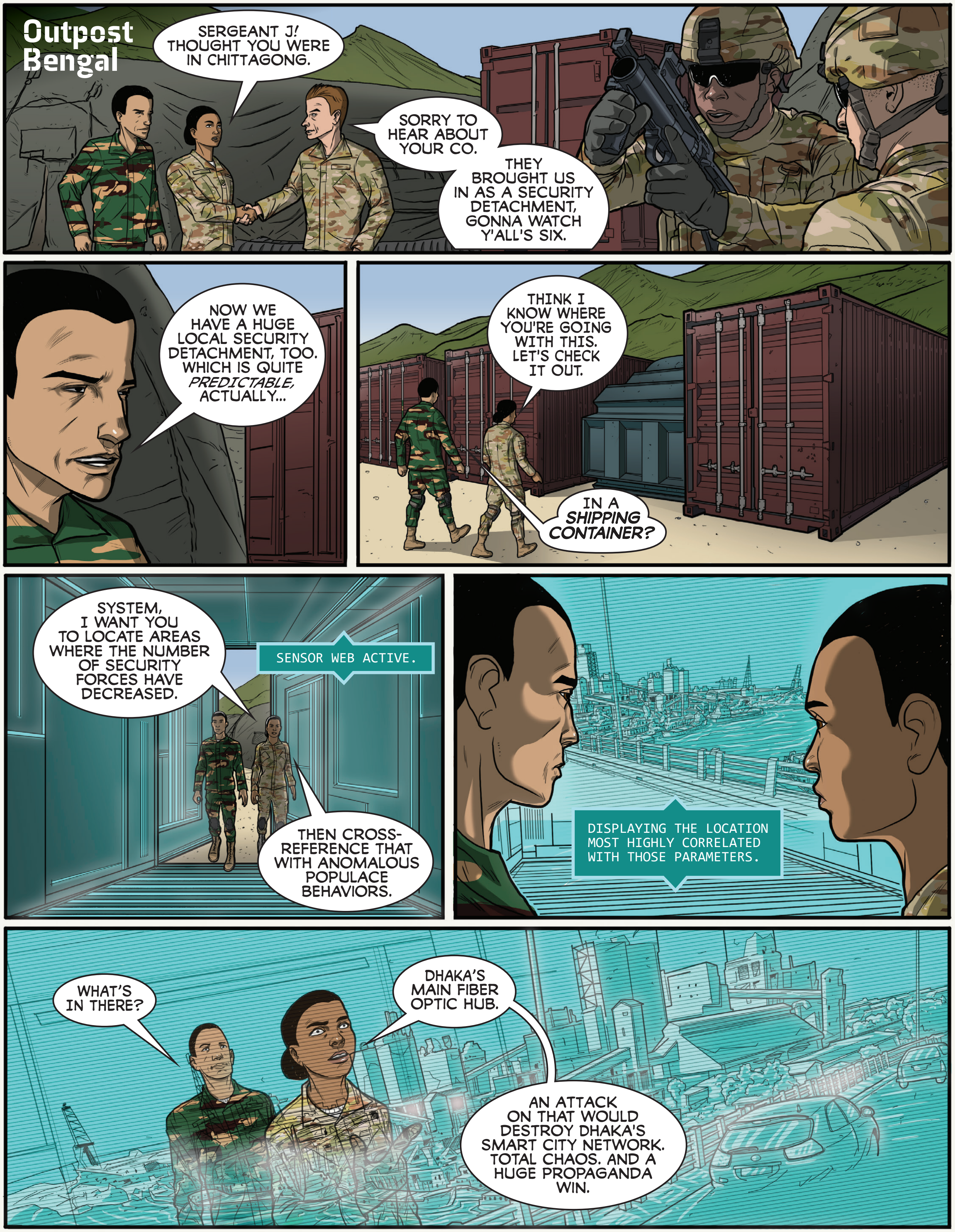
After transitioning from a garment-based economy to the wearable tech industry, the country has grown wealthier and undergone numerous reforms. At the same time, they have lost 18 percent of their southern landmass to rising seas, and in 2033 they were struck by the most **devastating cyclone** in decades.

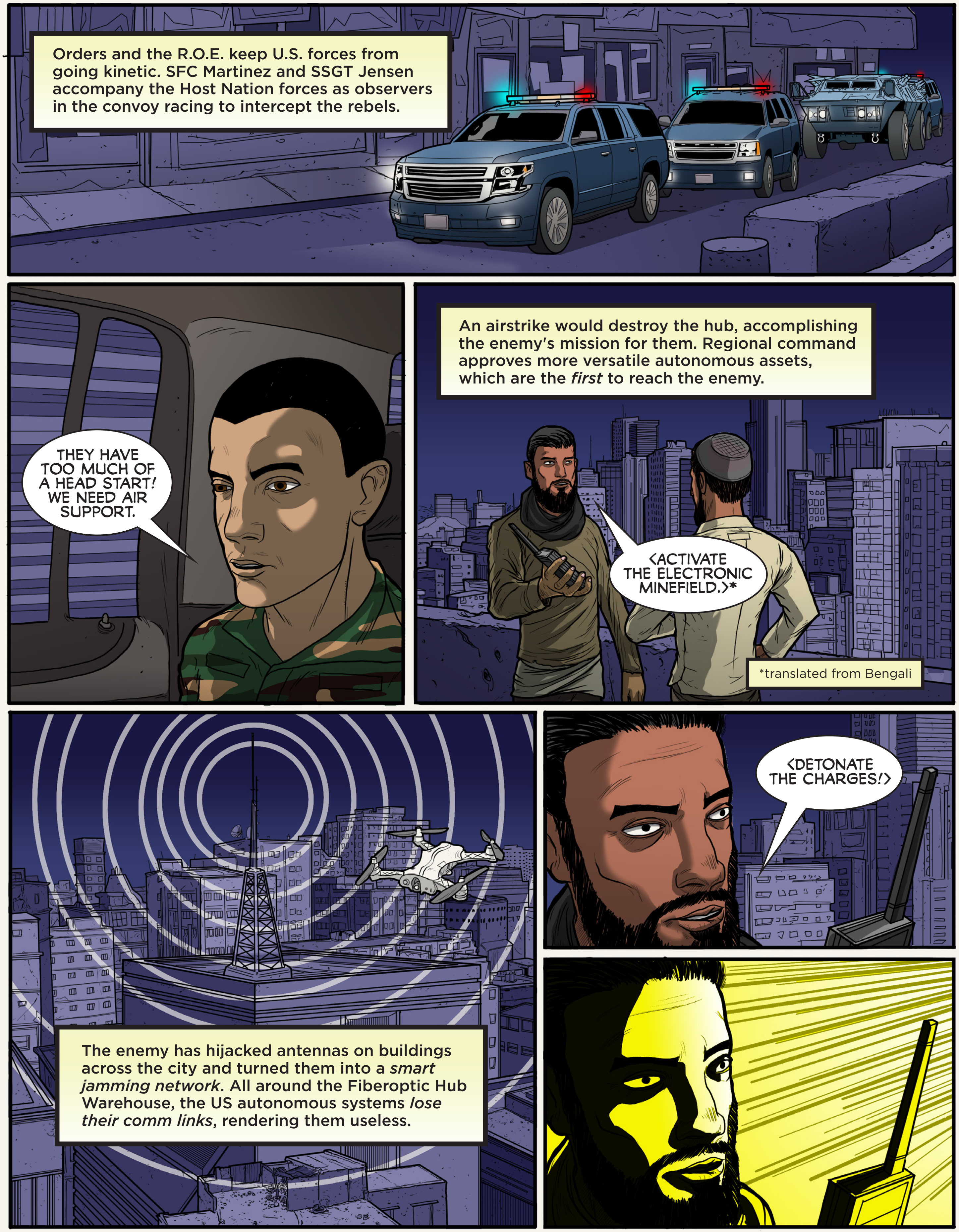
China-backed rebels took advantage of this disaster and launched a campaign to seize control of the country. A US-India coalition rushed to the aid of the legitimate government, and while they consistently win kinetic battles, they are losing the propaganda war. Thanks to the rebels' aggressive disinformation campaign, **many Bangladeshis blame the US** for the destruction and chaos.

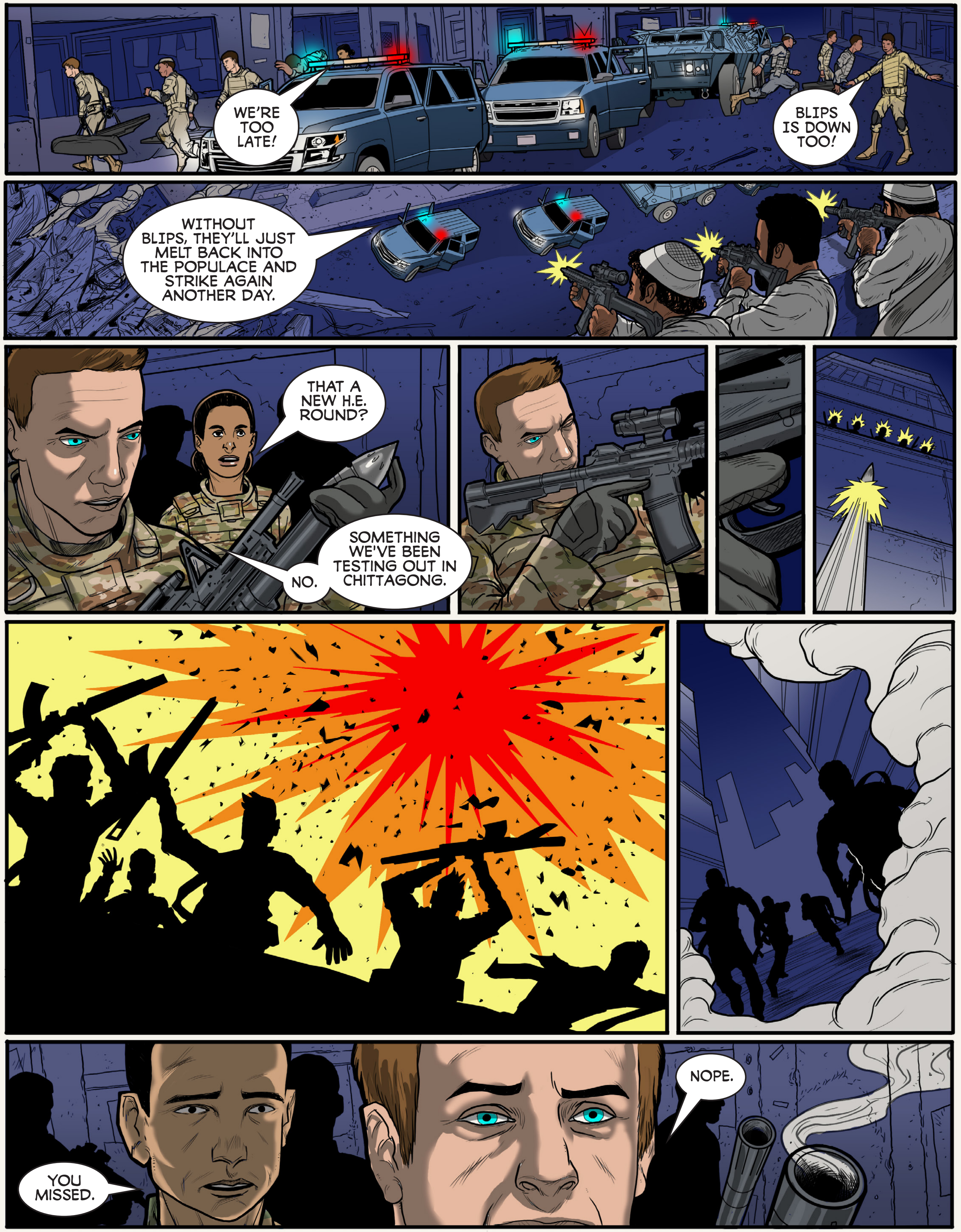
In the midst of all this, the US has deployed the 2nd Security Force Assistance Brigade to the capital city of Dhaka to train, advise, and assist their Bangladeshi Army counterparts.

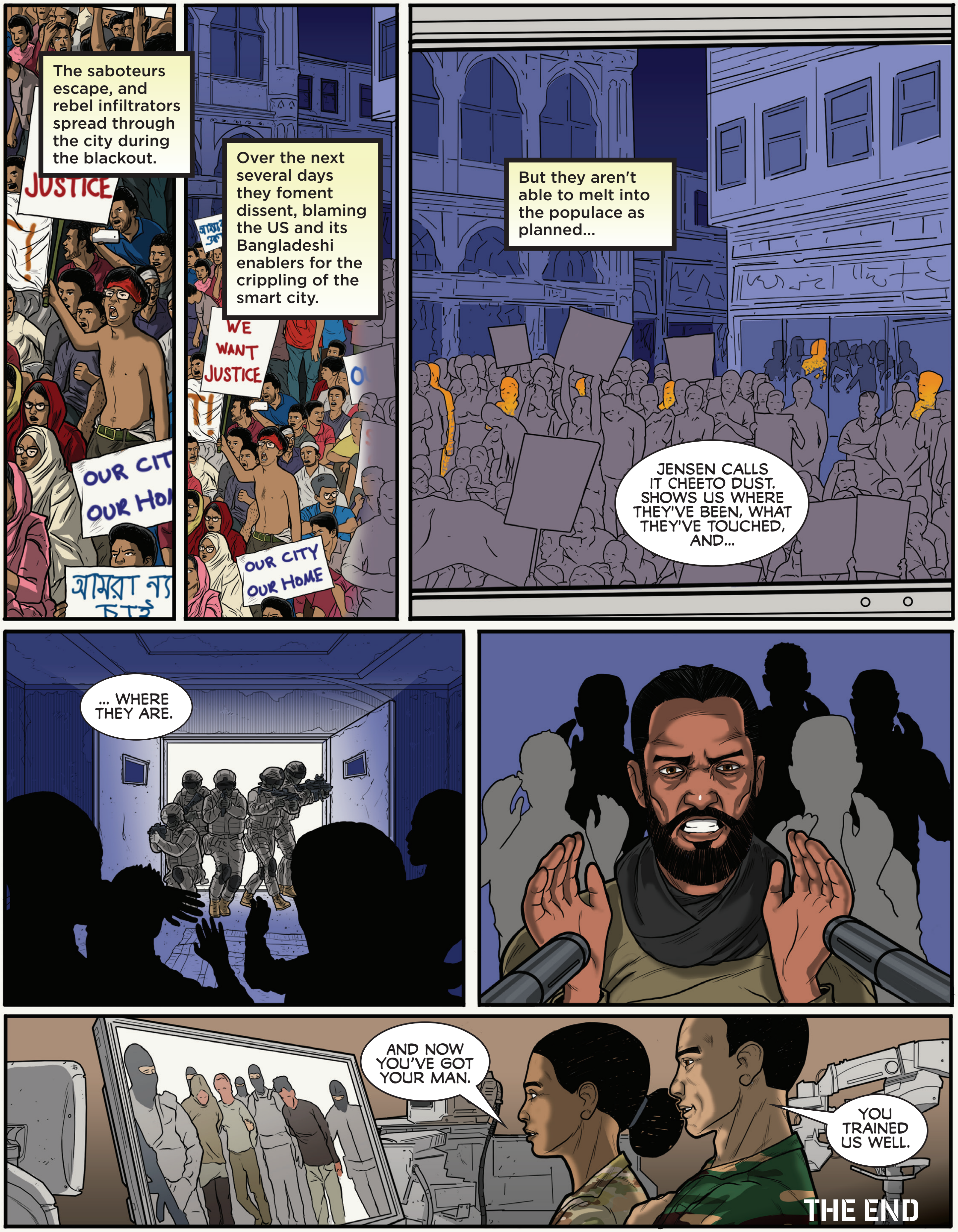
Not long after their arrival, **rebels attacked the 2nd SFAB** and their partners with a **kamikaze drone** attack on the Joint Military Installation Outpost Bengal...


Outpost Bengal - Field Hospital
2035
On the outskirts of Dhaka, away from the urban sprawl. A US, Indian, and Bangladeshi Military field outpost recovers from a kamikaze drone attack...
HE-- HE SAVED MY LIFE...
WHOEVER DID THIS CAN'T BE FAR. COMMERCIAL DRONES HAVE A LIMITED RANGE, AND SO DOES THE EMP PULSE THAT DISABLED THE DRONE GUNS.
THE ATTACKERS ARE PROBABLY HERE IN DHAKA.
THERE ARE **TEN MILLION** PEOPLE IN THIS CITY, SFC MARTINEZ. HOW WILL YOU FIND THEM?
BLIPS, LT KHAN. SMALL SENSORS THAT CREATE A SENSOR WEB TO TRACK MOTION AND PATTERN OF LIFE DATA.
WE'VE BEEN DISCREETLY PUTTING THEM IN STREET LAMPS, TRAFFIC LIGHTS, AND PUBLIC HUBS ALL OVER THE CITY.
NOT TO MENTION THE ONES PLANTED BY CONTRACTORS BEFORE WE ARRIVED IN-COUNTRY.


Outpost Bengal
SERGEANT J! THOUGHT YOU WERE IN CHITTAGONG.
SORRY TO HEAR ABOUT YOUR CO.
THEY BROUGHT US IN AS A SECURITY DETACHMENT, GONNA WATCH Y'ALL'S SIX.
NOW WE HAVE A HUGE LOCAL SECURITY DETACHMENT, TOO. WHICH IS QUITE *PREDICTABLE*, ACTUALLY...
THINK I KNOW WHERE YOU'RE GOING WITH THIS. LET'S CHECK IT OUT.
IN A ***SHIPPING CONTAINER?***
SYSTEM, I WANT YOU TO LOCATE AREAS WHERE THE NUMBER OF SECURITY FORCES HAVE DECREASED.
SENSOR WEB ACTIVE.
THEN CROSS-REFERENCE THAT WITH ANOMALOUS POPULACE BEHAVIORS.
DISPLAYING THE LOCATION MOST HIGHLY CORRELATED WITH THOSE PARAMETERS.
WHAT'S IN THERE?
DHAKA'S MAIN FIBER OPTIC HUB.
AN ATTACK ON THAT WOULD DESTROY DHAKA'S SMART CITY NETWORK. TOTAL CHAOS. AND A HUGE PROPAGANDA WIN.

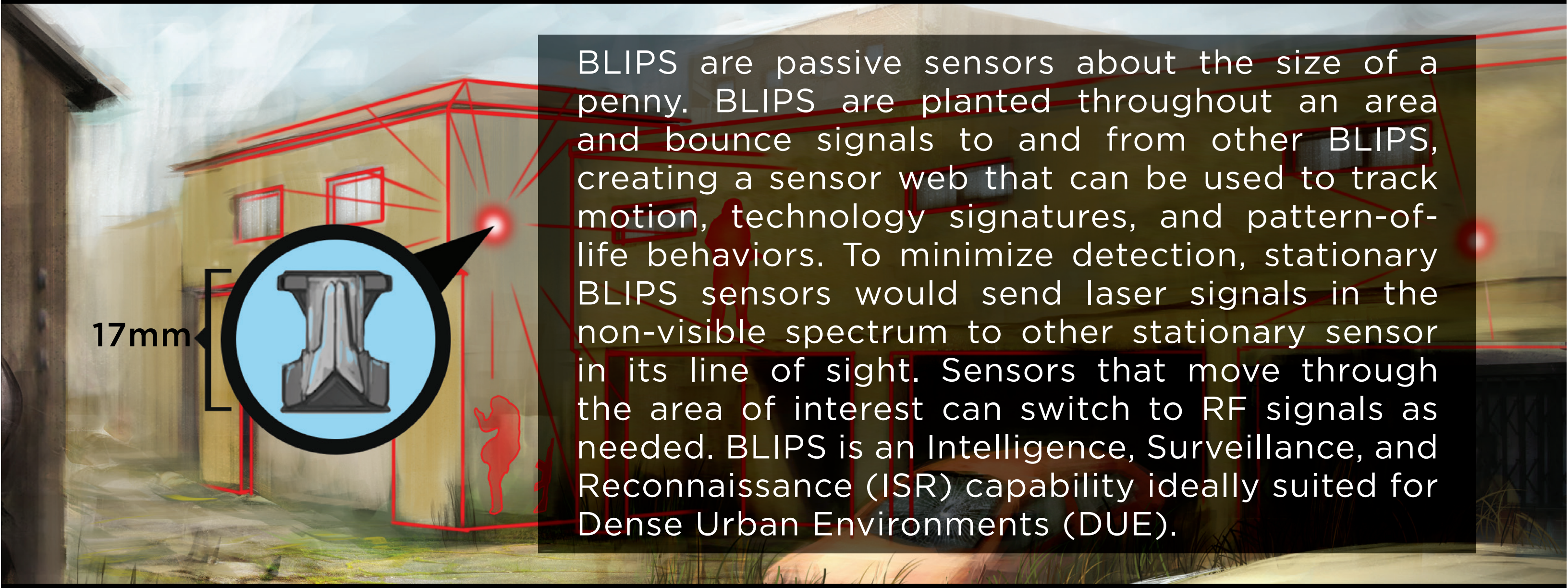

Orders and the R.O.E. keep U.S. forces from going kinetic. SFC Martinez and SSGT Jensen accompany the Host Nation forces as observers in the convoy racing to intercept the rebels.
THEY HAVE TOO MUCH OF A HEAD START! WE NEED AIR SUPPORT.
An airstrike would destroy the hub, accomplishing the enemy's mission for them. Regional command approves more versatile autonomous assets, which are the *first* to reach the enemy.
<ACTIVATE THE ELECTRONIC MINEFIELD.>*
*translated from Bengali
The enemy has hijacked antennas on buildings across the city and turned them into a *smart jamming network*. All around the Fiberoptic Hub Warehouse, the US autonomous systems *lose their comm links*, rendering them useless.
<DETONATE THE CHARGES!>


WE'RE TOO LATE!
BLIPS IS DOWN TOO!
WITHOUT BLIPS, THEY'LL JUST MELT BACK INTO THE POPULACE AND STRIKE AGAIN ANOTHER DAY.
THAT A NEW H.E. ROUND?
NO.
SOMETHING WE'VE BEEN TESTING OUT IN CHITTAGONG.
NOPE.
YOU MISSED.


The saboteurs escape, and rebel infiltrators spread through the city during the blackout.
JUSTICE
OUR CIT
OUR HO
আমরা ন্য
চাই
Over the next several days they foment dissent, blaming the US and its Bangladeshi enablers for the crippling of the smart city.
WE WANT JUSTICE
OUR CITY OUR HOME
But they aren't able to melt into the populace as planned...
JENSEN CALLS IT CHEETO DUST. SHOWS US WHERE THEY'VE BEEN, WHAT THEY'VE TOUCHED, AND...
... WHERE THEY ARE.
AND NOW YOU'VE GOT YOUR MAN.
YOU TRAINED US WELL.
THE END

BLIPS

Battlespace Low-profile Integrated Perception Sensors



BLIPS are passive sensors about the size of a penny. BLIPS are planted throughout an area and bounce signals to and from other BLIPS, creating a sensor web that can be used to track motion, technology signatures, and pattern-of-life behaviors. To minimize detection, stationary BLIPS sensors would send laser signals in the non-visible spectrum to other stationary sensor in its line of sight. Sensors that move through the area of interest can switch to RF signals as needed. BLIPS is an Intelligence, Surveillance, and Reconnaissance (ISR) capability ideally suited for Dense Urban Environments (DUE).

SUGGESTED CONOPS

This capability is best suited for covert forces and unconventional warfare.

There are multiple ways in which BLIPS could be distributed. They can be planted by their users, unknowingly distributed by others, emplaced in municipal objects, such as traffic lights, or embedded in commercial products, such as Wi-Fi extenders. If users are working with local governments, BLIPS could be installed on a number of sites (camera systems, trash cans, telephone poles, etc) by operators disguised as maintenance personnel. The more BLIPS are placed in an environment, the better the ISR outcome for a given networked area.

Each BLIPS ingests data, then transmits it to covert mobile hubs, such as a city bus, when the mobile hub passes within a given threshold. The mobile hubs, which can hold more data, then transfer the information to a stationary, terminal hub from which the user collects the entire network's data.

In a city, BLIPS could capture the activity of smart tech nodes throughout the networked area. The analysis of a populace's signal types, tech usage, and behaviors allows the user to identify and tag bad actors vs. non-combatants. The sensor web would create a sonar-like reading of the networked area, which could be turned into a 3D virtual recreation of the entire city for users to see and analyze. The massive amount of data generated by a BLIPS network should be shared with intelligence units for Processing, Exploitation, and Dissemination (PED).

BLIPS are an invasive form of surveillance with social implications that must be considered.

KEY ATTRIBUTES

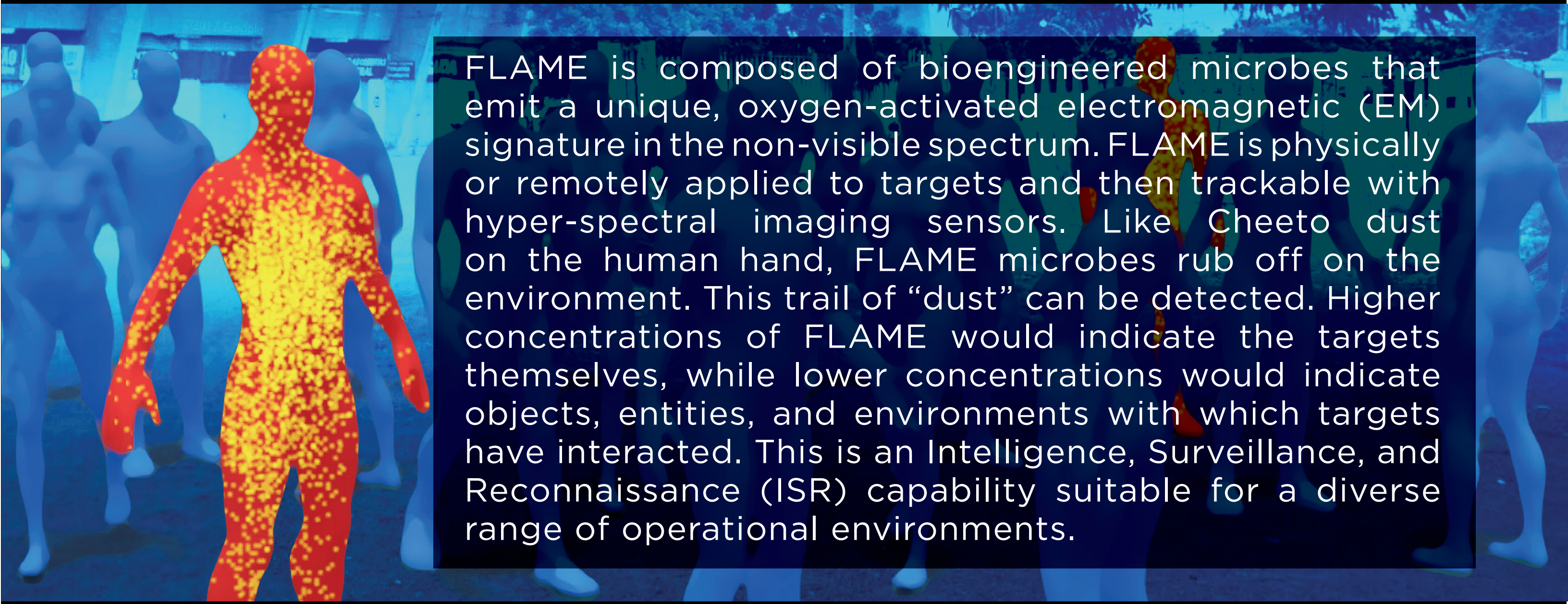
- The BLIPS network senses and communicates with laser and RF signals. Humans and artificial intelligences must collect, share, and analyze the data collected. Processing time will be constrained by the human and computing power available to the user.
- Each BLIPS laser-emitter has a maximum effective range of 3 kilometers, and its RF transmitter has a range of 2 kilometers. Sensor must have line of sight with another sensor for laser signal exchange.
- Each BLIPS is a passive device requiring no operator. However, operators must distribute or emplace the BLIPS devices, and emplace and maintain the hubs that transmit and store the data collected by each BLIPS.
- BLIPS are powered by untraceable polymer batteries and have a lifespan of 3-4 weeks.

HOW FAR IN THE FUTURE?

This technology will likely become feasible in the 2035-2045 timeframe. The main hurdle in reaching the described capability are the current limitations of batteries, especially at such a small size. This capability assumes continued advancements in power sources and battery miniaturization.

FLAME

Forensic Luminescent Active Microbial Emitter



FLAME is composed of bioengineered microbes that emit a unique, oxygen-activated electromagnetic (EM) signature in the non-visible spectrum. FLAME is physically or remotely applied to targets and then trackable with hyper-spectral imaging sensors. Like Cheeto dust on the human hand, FLAME microbes rub off on the environment. This trail of "dust" can be detected. Higher concentrations of FLAME would indicate the targets themselves, while lower concentrations would indicate objects, entities, and environments with which targets have interacted. This is an Intelligence, Surveillance, and Reconnaissance (ISR) capability suitable for a diverse range of operational environments.

SUGGESTED CONOPS

FLAME could be applied in a number of ways, though three primary methods are proposed. In the first method, a covert user applies it to targets (vehicles, supplies, etc) with an aerosol spray.

A second method requires the user to introduce FLAME-laced materials into the enemy supply chain. Standard packing tape, for example, could be laced with FLAME, and the users of the packing tape would not be able to detect this with the naked eye. Supply-chain applications of FLAME would provide useful insights into targets' logistics, providing snapshots of their interactions with each other and with their environment.

The third method is including FLAME in lethal or non-lethal rounds fired at the enemy, such as a grenade or mortar round. When these rounds strike a target or explode, FLAME particles would land on enemy personnel or vehicles and become activated by exposure to the air. In this case, FLAME could be used to track enemy units after an engagement.

FLAME utility could be increased by creating a different EM signature (or "frequency hopping") for each application, i.e., microbes created to emit different wavelengths. This would allow for more accurate target identification and tracking.

KEY ATTRIBUTES

- The FLAME substance can be a solid or liquid solution that combines bioengineered microbes, their growth medium (food), and the delivery material.
- Oxygen-activated, stored in vacuum-sealed container.
- On activation, the unique EM signature is emitted for 90 days.
- The range of the EM emission is virtually unlimited. The ability to detect, recognize, and identify targets on which FLAME has been applied depends on sensor line of sight, sensor sensitivity, ambient EM saturation, and amount of dusting.

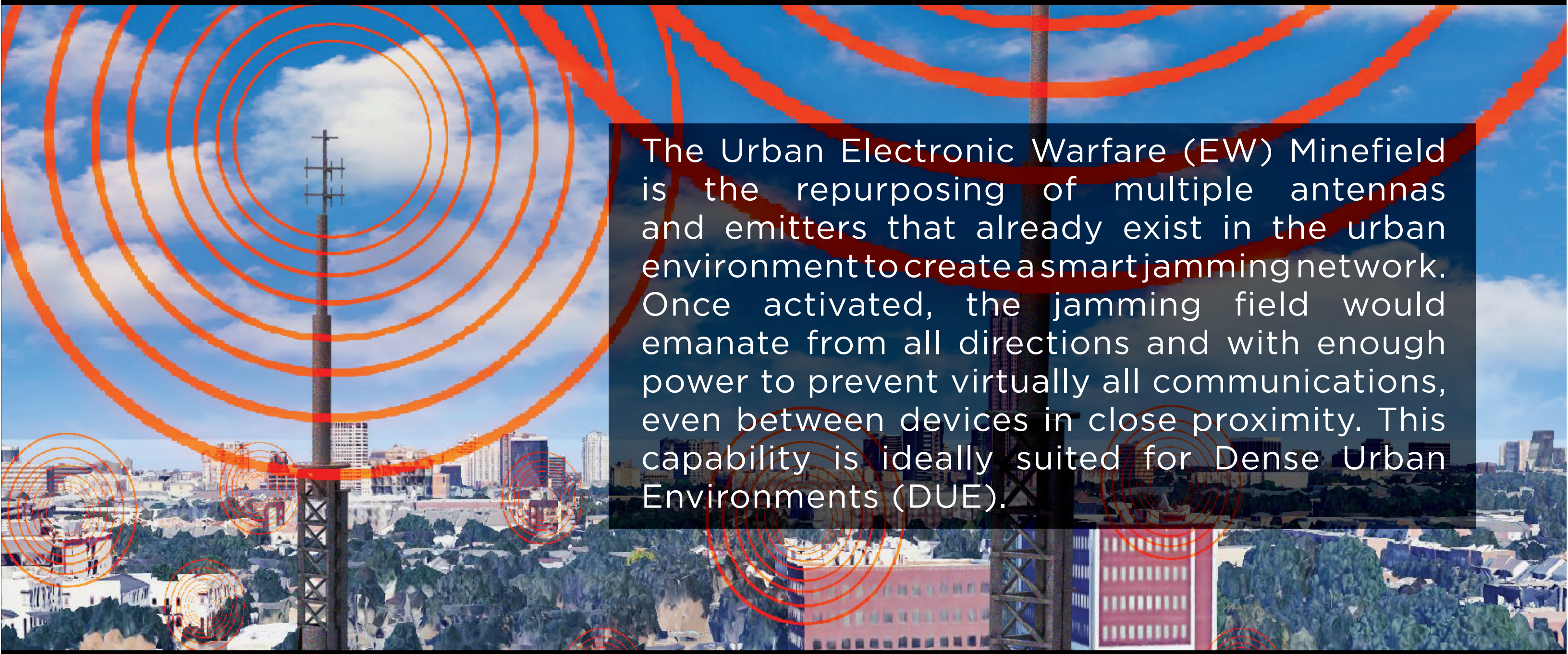
HOW FAR IN THE FUTURE?

The US Air Force, US Navy, and NSF already fund research on bioluminescence in the hope of military applications.

Researchers have successfully inserted bioluminescent genes into animals to make them fluoresce, and work continues into development of new bioluminescent proteins. FLAME requires the engineering of innocuous, enduring trace microbes that persist without over-colonizing their targets.

EW MINEFIELD

Electronic Warfare Minefield



The Urban Electronic Warfare (EW) Minefield is the repurposing of multiple antennas and emitters that already exist in the urban environment to create a smart jamming network. Once activated, the jamming field would emanate from all directions and with enough power to prevent virtually all communications, even between devices in close proximity. This capability is ideally suited for Dense Urban Environments (DUE).

SUGGESTED CONOPS

A dedicated team or unit would repurpose antennas, such as cell sites/towers, either by altering the hardware or by hacking the software.

The force implementing the EW Minefield would equip themselves with dedicated land lines and other non-jammable communication means, preventing any other force from communicating in the environment.

This would disrupt not only command and control, but also vehicle-to-vehicle communication and links to autonomous systems, greatly degrading their effectiveness.
EW Minefield activation would be integrated with battlefield command to enable rapid and effective tactical operations against the degraded enemy.

In *CITY OF SHADOWS*, the EW Minefield is used by fictional adversaries. This capability could of course be developed and used by US forces.

HOW FAR IN THE FUTURE?

This capability is feasible in the near future with a few enabling developments in science and technology. These are continued wireless and RF infrastructure building, more emitting systems linked to the internet (allowing for software vs hardware hacking), cost decreases, and easily transportable broad spectrum jamming or emitting hardware that can be setup and attached to various antennas and left there.

KEY ATTRIBUTES

- Broad-spectrum jamming.
- Installed and activated by human operators.
- EW Minefield Systems would share a common infrastructure built on the baseline of exploiting mobile phone systems hardware and software, i.e., cell sites/towers. Individual systems would be further specialized to the nodes available in the local urban environment.
- The duration of the jamming field would last as long as the majority of nodes in the jamming network has power.
- If compromised, jamming nodes would self-destruct (if hardware) or erase sensitive data (if software), known as zeroization in cryptography. This prevents recovery or use of the technology or data by the enemy.

Discover more innovative concepts, bold ideas, and new technologies at:
https://futures.armyscitech.com/