ARMY CYBER INSTITUTE AT WEST POINT PRESENTS:

QUANTUM WINTER

WRITEN BY: BRIAN DAVID JOHNSON CREATIVE DIRECTION: SANDY WINKELMAN ART: DON HUDSON & KINSUN LOH



BUILDING A BETTER, STRONGER AND MORE SECURE FUTURE FOR OUR ARMED FORCES

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. Our story does not shy away from a dystopian vision of tomorrow. Exploring these dark regions inspires us to build a better, stronger, and more secure future for our Armed Forces.

> Lt. Col. Natalie Vanatta Academy Professor U.S. Army Cyber Institute

The views in this graphic novel are those of the author and do not reflect the official policy or position of the Department of the Army, DOD, or the U.S. Government.

QUANTUM WINTER

Adversaries have beaten the U.S. to the punch, acquiring quantum computing capabilities well ahead of the technological world's expectations. The ramifications of the enemy's advantage in computational power are felt by a team of U.S. Army technical soldiers during a tactical mission. The team suffers the chaotic effects of the enemy's advantage, leaving them immobilized by enemy fire and unable to communicate for fear of being more precisely located. Outside, the nation's power grid is under constant cyber attacks, producing persistent rolling brown outs. With no encryption, banking systems are hacked, destabilizing the economy and inciting civilian riots in major urban centers. The nation is frozen in a "quantum winter," unable to defend itself, experiencing the prolonged effects of losing the technological race in computational power.









AFTERWORD

Institutions within nation-states continue to aggressively pursue the achievement of quantum supremacy. Most of these endeavors aspire to solve some of the world's most difficult mathematical problems. One thing holds true, whichever nation possesses "quantum supremacy" first has the capability to shift global hegemony in their favor. Quantum computing gives the U.S.' adversaries the capability to crack the most sophisticated encryption algorithms, protecting our national security information. This capability will enable its possessors to wreak chaos and havoc on the information networks of any nation that opposes its will.

What can the U.S. do to assure the security of information contained within our national information infrastructure if we lose the quantum race? How do we pursue encryption research designed to address information security in the "post-quantum" world? What battlefield systems could be emplaced to counter the effects of a "quantum winter" from enemies possessing this advantage?

As illustrated in this story, enemies with quantum computing capabilities could render U.S. military units completely isolated, confused, and powerless. The need to develop new "quantum proof" encryption algorithms has never been greater. While quantum computing promises a lot of good for the world, it also poses an existential threat to our national security.

