# The New Technology Cold War

It's amazing to think that Generation Z doesn't understand what the Cold War was — all those decades lived under the threat of nuclear annihilation, the unbelievable tension of the Bay of Pigs Fiasco under the Kennedy administration, the constant paranoia generated by the idea that our institutions had been penetrated or compromised by foreign agents of the Soviet Union — and if you were born in Generation X, as I was, then the Cold War was a part of your life right up until you were in your early twenties.

The Cold War was an ideological conflict between the West and the Soviet Union, and the term *Cold War* refers to the fact that there was no direct exchange of bullets or bombs between the two principal parties in the Cold War. The Cold War was fought entirely by proxy and by propaganda and by the never-ending arms race. It finally ended when President Ronald Reagan commenced the Space Race. The then-leader of the Soviet Union, Mikhail Gorbachev, folded his hand at the poker table of this Cold War and said *no more*. He slowly began to dismantle the Soviet Union through two programs known as perestroika and glasnost.

Even though Generation Z did not experience the Cold War, cold wars have become endemic to the human experience. We no longer fight these cold wars between nation-states, but we still fight them. The characteristics of a cold war are a constant escalation of armaments to keep up with the enemy, then the world of technology is in a constant state of cold war, and just like the war that coined the phrase, in these modern cold wars no bullets are fired, and no missiles are launched, but a constant state of conflict by proxy exists, where one of the major proxy agents is the ever advancing world of the bot. Russia and the United States may have defined the concept of conceptual war, as no combat aggression, but it always existed, and its present expression is technology.

## A New Cold War

We are in fact in a non-nation state cold war now in the intangible, amorphous, and mysterious world of networks and technology. Many of the elements of the Cold War are still in place. The Cold War was perpetuated by military-industrial complexes in both the Western world and the Soviet Union. Each had to escalate their game to meet the capability of the other. This could be defined as the signature of a cold war, mutual expenditure, and mutual evolution in the technology used in the war. This is precisely what is going on in the technology sector now. The parameters of engagement in this cold war are privacy, security, the continuity of digital commerce, digital markets, digital banking, and prevention of fraud and theft according to a safe digital market space.

This cold war is taking place between one party which wants to maximize the use of computers and networks for commerce and transactions and another party which wants to make that as difficult as possible for any number of reasons. Some of these reasons are ideological — like the original Cold War — in this new cold war the ideology might be sentiments of anti-capitalism, anarchism, and anti-monopoly. Some reasons are theft and illicit gains, and this too was a characteristic of the original Cold War, which was very profitable for the companies selected to fight the war through weapons design and manufacture. And some reasons are lacking reason altogether. These we might call, in the colloquial, *smash and grab* reasons, no different from looting during civic unrest.

## Hackers are the New Spies

Similar to the spy of the original Cold War — think John le Carre, Tom Clancy, and Ian Fleming — a kind of romance has emerged around the hacker. In some instances, the hacker is a hero. If a hacker can destroy enemy infrastructure, then he’s a hero to the side that employs him or her. If the side we are on is violated by a hack, then that particular hacker is a villain. You can’t live with hackers, and you can’t live without them. We need them to save us from the other hackers, just like the spies of the original Cold War.

Similar to the nation-state in the Cold War, it’s impossible to run a large scale network or business without a security team, just like the CIA, MI6, and the KGB were needed so too are the myriad experts, consultants, and technology. These teams need resources and personnel. The resources take the form of software and technology and the personnel who advise on the purchasing of these products and install, configure, and maintain them. And, like all wars, it’s the little people who pay for it. In the original Cold War, the Western taxpayer footed the bill. In this new cold war, another person foots the bill. One way or another the cost of this cold war between the people who want to hack transactions on the internet, defraud people of their identities and their purchasing power, and the forces that want to protect it, are paid for by the common person we call the consumer. The technological cold war is paid for by the consumer because the cost of securing networks is a value-added cost to the products being sold online.

## Tool of the Trade

In the profession of the digital fraud artist and the digital thief, the go-to tool is the bot. The word bot is just a catchy abbreviation of the robot. The computer world likes to produce its own language that is highly colloquial, almost a kind of technology hip-hop language. In the case of network security, a bot is an application that can perform any number of tasks. At their inception, bots were fairly one-dimensional. If you remember the Cold War, cast your memory back to the beginning of video games. Do you remember Pong? Two paddles that could move vertically on a TV screen to bounce back a white dot. It was basically ping pong on your television set. Take a look at gaming today. It’s merged with virtual reality. There are tournaments in which the top players are millionaires and celebrities, like pro athletes in their own right and their own space, albeit digital space. It can take almost as long to become proficient at certain video games that are competition-worthy as it can to perfect something like figure skating or another professional sport. It all started with Pong.

The same is true for bots. The very first version of bots was like a dog that could fetch a stick and return it to you, but just like video games bots have advanced enormously. The main reason for this is artificial intelligence (AI). Coupled with this is machine learning (ML). There have also been significant advances in automation technologies. Here’s a short encapsulation of what bots can do now as compared to the original bots which were just fetching a stick. Bots now can interpret language. This is thanks to natural language processing (NLP). The algorithms associated with natural language processing have advanced to such a point that computers can talk now. This has produced bots that can communicate with us. Most of us have encountered them as virtual assistants or in some form of customer service.

The next big advancement with bots is their ability to learn. We classify this under the umbrella of machine learning (ML). But it's just learning the same way a human being learns. Children learn their social skills by interacting with their brothers and sisters, their mothers and fathers, and the other kids at daycare and school and then through to university and the workforce. It’s no different for bots now. When a bot is deployed in a certain circumstance it can grow and mature through the interactions it has with human users, and once again this is largely due to the advancement of the algorithms.

Bots also now can realize highly complicated and sequential tasks. Using the analogy of the dog fetching a stick and bringing it back, bots can now go get the stick, and do a circle, a backflip, run around a tree, bring the stick to your feet, then go get you a beverage from the refrigerator. It’s quite alarming the advancement in complex task realization that bots have achieved in the last few years.

One of the more pernicious advancements in bots on the security side of this technology cold war is the ability of bots to mimic human behavior. This means that certain things that only human beings could do can now be done by bots. The problem with this is that many of the security measures to verify that you’re dealing with a human being in an online transaction can now be mimicked by bots. For example, it used to be that only a human being could solve a captcha. This is no longer the case. Bots are now able to solve most captchas now. This is one of the major fronts in the technology cold war. The ability of vendors to operate online and feel assured that they are dealing with human beings, and on the consumer side, the confidence that any transaction they perform has enough security measures in it to prevent a bot from doing it, has been seriously compromised.

It's in the captcha space that the security threat of bot advancement is the greatest. Captcha stands for (Completely Automated Public Touring Test to Tell Computers and Humans Apart). You know them as those sometimes annoying little quizzes that pop up before you pass along to the next phase of accessing a website or completing a transaction, things like choosing all the buses from the pictures above. They have been fairly resilient for the last decade or so, but the cold war just keeps escalating. This is what most distinguishes this technology stalemate as a cold war. Just like the Soviets acquired nuclear weapons shortly after the West, every time there is an advancement in computer security the hackers take the very material used for the advantage, like ML and AI, and employ it in their bots.

Here is just a short list of the things bots have been able to accomplish in a few short years. Optical character recognition (OCR) by automated bots which can now employ OCR technology to interpret the characters in a captcha image. This is a game changer. One of the few sure ways to distinguish between a bot and a human being in the last decade has been the selection of images, which, up until recently, has been the unique province of human beings looking at a computer screen. No more. Now the bots can do it. If the OCR was not enough, now ML has algorithms that can recognize the characteristics of an image and correctly select the sought after image. Finally, there are now pre-processing attacks by bots in which the bots may attempt to manipulate the images in the captcha matrix before processing them, thus enabling the bots to recognize the images and solve the capture riddle.

Online commerce is not going to go away. Hackers and digital fraudsters are not going to go away. If you’re an online vendor, you’re going to have to choose an intelligence team to aid you in your online security. You can’t go it alone. During the actual Cold War intelligence was shared by all NATO countries. In the world of online security and the ongoing cold war in this technological landscape, only a handful of security teams stand out. Google made a splash when they upgraded captcha to reCAPTCHA©, but even this has fallen by the wayside. The only thing that keeps up with what is happening on the hacker side is hCaptcha™ by Intuition Machines, supported by a team of leading software engineers in artificial intelligence and machine learning, producing a constantly evolving product that meets the needs of this technological cold war.