DAILY RECKONING

The Greatest Government-Backed Bull Market of Our Lifetime

BYRON KING

The Greatest Government-Backed Bull Market of Our Lifetime

Dear *Daily Reckoning* Reader

There are undeclared wars going on all over the world today.

You won't hear about these wars on the news, though some of the world's leading countries are involved. In fact, it's very likely that the U.S. is involved in at least one of these "wars" right now.

That's because these conflicts are operating in the fifth domain of war: cyberspace — the latest battlefield after land, sea, air and space.

Descriptions of cyberwarfare read more like science fiction than the annals of military history: Offensives jump off at the stroke of a key. The sentries are firewalls, encryptions and passwords. **Viruses drop behind enemy lines like guerillas and sow confusion.**

It's a whole new way to wage war, and one that some predict will dominate international relations in coming decades. In fact, the increasing importance of cyberwarfare could well shake up the existing balance of military power around the globe.

How can politicians and generals resist? With plausible deniability, it's as close to war without risk as the military can get. Need to shut down a rival country's secret weapons program but can't penetrate their airspace undetected? **Drop a virus instead of a bomb!** That's the kind of option policymakers and warriors have on the table now. It's a whole new ballgame.

Indeed, some experts say the wars of the future will be fought only with Special Forces operators and computer programmers. However, until we figure out a way to profit from the Navy SEALs, I'll stick to talking about the latter — cyberwarfare and the profit opportunities it gives you, the investor.

War in the "Fifth Domain"

Cyberwarfare is a $55 billion industry. It's also America's fastest-growing industry, set to double in the next 12 months. One recent study characterized cyberwarfare as "the ultimate asymmetric weapon" — I like "the fifth domain of war" better.

One of the biggest challenges that emerges in taking war to the fifth domain is that cyberwarfare capabilities offer a powerful and immediate force multiplier for rogue states. Countries that previously posed little threat when judged by conventional military standards, such as Iran, now pose much larger ones.

Iran's conventional military doesn't rank in the world's top 10. Despite having more than a million men under arms and several thousand armored fighting vehicles and combat aircraft, it's doubtful that it could survive a conventional war.

Yet a recent cyberwarfare study by the Atlantic Council, a beltway think tank, classified Iran as a tier-three cybermilitary. That means it's capable of causing significant harm to civilian networks within the U.S., if not in the government. What a jump in capabilities for this fourth-rate military power halfway across the world!

Meanwhile, Iranian hackers have been poking for holes in the U.S. cyberinfrastructure. If they ally with the Syrian Electronic Army, they could launch several cyberattacks — many of which would affect private businesses — particularly banks.

Currently, JP Morgan spends $200 million on cybersecurity every year. And the bank's CEO, Jamie Dimon, told shareholders that number "will grow dramatically over the next three years." It's indicative of the new correlation between U.S. involvement overseas and the consequences businesses face for it back home.

Cyberstrike capabilities have leveled the battlefield. And the scrappy countries are holding more bargaining chips. "One of the risks is that you've got Iran talking to Russia," says James Lewis, a fellow at the Center for Strategic and International Studies. "You have Iran talking to North Korea; you've got the Syrians talking to Iran." True enough, but an even bigger threat may be looming...

China's Drone Obsession

As if relatively small rogue states weren't bad enough, now China is getting in on the action. Already the world's third most powerful military

continue...

(according to Business Insider), China recently jumped into the cyberwarfare game feet first. Their target? U.S. drone technology.

"For almost two years," writes Edward Wong in *The New York Times*, "hackers based in Shanghai went after one foreign defense contractor after another, at least 20 in all. Their target, according to an American cybersecurity company that monitored the attacks, was the technology behind the United States' clear lead in military drones."

The U.S. currently has the most sophisticated drone technology on the planet, and with 7,000 unmanned aerial vehicles (U.A.V.) at its disposal, it also has the world's largest arsenal. But China wants to change all that, and the most effective way for it to do that is through cyberspace.

"For the Obama administration and American business executives," says the *Times*, "no method of Chinese technology acquisition is more worrisome than cyberespionage."

With that in mind, it's easy to see where the Pentagon will begin to focus its attention… and its budget (more on that in a minute). But despite all the developments in Iran, China and other rogue states, the Pentagon is far from licked…

The New Face of Collateral Damage

The practical anonymity that makes cyberwarfare the perfect way for rogue states to attack the U.S. and its allies also makes it the perfect weapon for democratic countries too. Now, without a mandate for "boots on the ground" warfare or U.N. approval, they can launch pre-emptive or retaliatory strikes against these threats. They go from being front-page news to wink, wink, nod, nod.

Most recently, it's become known that the destruction of Iran's latest nuclear testing facility was carried out in the fifth domain by a virus call "Stuxnet," reputed to be a joint operation between the United States' NSA and CIA and Israel's military. This was the first time a virus did significant physical damage to a military facility.

Unfortunately, Stuxnet has, in some respects, backfired. The computer worm broke out of Iran's nuclear facilities, perhaps through an infected laptop that was connected to the Internet. The software, designed to propagate virally, spread beyond its intended target and across the Internet at large, infecting private computers and networks. Since then, it has spawned imitators who have exploited its code base for new attacks.

Pay attention: This is what collateral damage will look like in the new domain of war…

In May of this year, U.S. intelligence sources confirmed a cyberintrusion into one of the most sensitive databases of the nation's physical infrastructure — the U.S. Army Corps of Engineers' National Inventory of Dams (NID).

This single database details all the vulnerabilities of every major dam in the country — about 8,100 dams across our nation's waterways. Now imagine a cyberattack on the network of a single major dam. Such an event could easily compromise the network and allow for malicious code to be planted inside — code that could later open the floodgates or lock them in place. **Within minutes, the valley below could flood, with unimaginable consequences, including loss of property and life.**

While the intrusion at the NID was discovered in May, intelligence reports show that the database was actually penetrated in January, five months before it was discovered. Further investigation suggests that this intrusion came from unauthorized users based in China. Of course, this raises new fears. Officials are now concerned that China may be preparing to conduct a future cyberattack on the national electrical power grid.

Some nations may even enlist the help of criminal organizations to carry out their cyberattacks. President Obama's former cybersecurity coordinator, Howard Schmidt, recently said there was evidence that foreign governments were even taking kickbacks from local cybercriminals that target U.S. corporations — it's a "quid pro pro for letting them operate."

Now a foreign state can opportunistically soften up its targets, with little use of traditional military resources, under a guise of deniability.

Who's the BOSS?

Of course, external threats aren't the government's only concern. Developing and perfecting facial recognition technology has been essential to the government's focus on *domestic* cybersecurity. And a recent development in biometric technology might be just what they're looking for…

According to a recent report on biometricupdate.com, "The U.S. Department of Homeland Security will test its crowd-scanning facial recognition system, known as the Biometric Optical Surveillance System, or BOSS, at a junior hockey game."

What does this have to do with cyberwar? Well, as the article continues, "a $5.2 million contract for BOSS was awarded to Electronic Warfare Associates, a U.S. military contractor."

continue…

So while the clear applications are for wide-ranging facial recognition at places like airports and border crossings, there may be even more, military-focused applications to come online in the very near future. And that will be a nice bit of technology for the Pentagon to have in its back pocket, should other countries begin to stockpile their own cybersecurity technologies...

Prepare for a "Cold" Cyberwar

Since the end of the Cold War and demise of the Soviet Union, there's been a tendency for the public to think that there are no more "arms races" in the world. That idea is entirely wrong...

In fact, there are new arms races in many respects, across the world. Some of the "deliverables" still include big ships and submarines (think China), fighters and thundering bombers (China again) and missiles (China, North Korea, Iran and more).

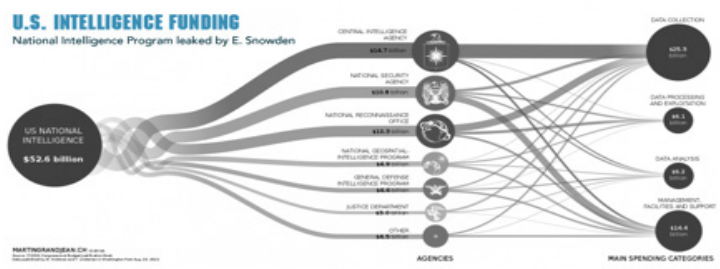
But much of the next arms race is well hidden — in cyber-labs, and in research facilities that work on assembling super-complex electronics and optics into remote drones and directed energy systems.

It's all happening. And business is — if you'll forgive the pun — "booming."

The Washington Post recently released information it received from the renegade whistle-blower Edward Snowden about the U.S. intelligence community's funding for secret projects. It's been dubbed the "black budget." What they found was startling…

The 178-page report details exactly how the intel budget will be portioned out — I'm talking the who, what, when, where, etc. In case this isn't clear: **This information has never — I repeat, never — been made public before!** At least it's never been intentionally made public before. Let's focus on two points:

1. The CIA — the spearhead of intel "offensives" overseas — which received just 11% of intel money in 1994, will receive a whopping 28% of the "black budget" in the next fiscal year! That's even more than what the NSA will get.



Click here to Enlarge

2. **Cyberwarfare-related activities will receive more than $4.2 billion,** according to the Post's breakdown. That's nearly 10% of the whole intelligence community's budget! My, how times have changed from the early days of the Internet.

The bottom line is that our military planners see the next big threat coming in the form of an attack on the computers that run our country, and they're preparing. These revelations can and should move markets… At least if you're paying attention.

To expand its cybersecurity programs, develop new capabilities and shore up its network defenses — a $16.1 billion endeavor — the government is relying on private cybersecurity companies to do most of the heavy lifting. These firms — some tiny — have "the right stuff," to borrow a phrase, and they're for hire.

I've spent hours poring over these leaks, "Black Budget" details and declassified documents. I've been following the public companies that are best poised to gain from these massive outlays of our tax dollars, and I've whittled down a handful of ticker symbols. You can view all of the information here, free of charge. Essentially, it's a blueprint to investing in the "Black Budget". After all, the Pentagon is practically announcing where investors can earn fat returns on their money.

We ask you sign a disclosure form before we give you access… but it doesn't require you to open your wallet or give us your personal information. After you sign it, you'll be sent straight to my research. In all, I've listed seven defense contractors that I think are positioned to skyrocket from this $16.1 billion shift in spending. Simply click here to view the information on these defense contractors for yourself.

Regards,

Byron King for *the Daily Reckoning*

P.S. I recently examined another emerging story in the U.S. that I think will be just as lucrative, if not *more so*. What I discovered could bring about a new era of wealth and prosperity that puts the U.S. back on top. I'm talking about a growing industry that will create up to 5 million new manufacturing jobs and make a few savvy investors fabulously wealthy. And it's all happening right here, in the U.S. of A. Find out all the details on the story that will remake America, right here.