All.Net Analyst Report and Newsletter

Welcome to our Analyst Report and Newsletter

What happened to the cyberwar?

We have been told for years about how weak our cyber defenses are:

- The entire Western world could collapse under cyber-attack.
- The government cannot stop it and does not run it.
- All of your money and ability to use it could go away.
- You could be sent back to the dark ages with no water, power, etc.

Now we hear there is very active offensive cyber-warfare activity underway:

- Lots of attacks being launched by the Russian Federation and their allies.
- Targeting all manner of systems, companies, etc.
- Some just testing a capability, other actively exploiting

So why aren't we being wiped out?

I don't have a specific answer, but rather some speculation:

- According to some folks I know in large enterprises, they aren't seeing anything more or different than what they have been seeing over time anyway.
  - Perhaps any new attacks just aren't making a substantial difference compared to what was already going on.
  - Perhaps it is so stealthy that they just don't see it yet, and when it hits they will be helpless.
  - Perhaps the attackers are staying away from strong defenders and focusing on some specific strategic targets that don't have such strong defenses.
- According to my day-to-day life, the Western world has not yet collapsed from cyber attack.
  - Perhaps the Russian cyber capability, apparently like it's physical military capability, is more of a paper tiger than we imagined it was.
  - Perhaps our defenders actually know what they are doing, or at least they can run faster than the bear that's chasing them.
  - Perhaps the Russians are not going for the gut punch and just waiting and testing our resolve and capabilities before they actually do harm.

Or perhaps, the Fear, Uncertainty, and Doubt was just a sales pitch

I think there was and still is plenty of FUD and sales surrounding cybersecurity. And I try to fight it everywhere I see it. But I also think the potential for great harm remains real. The thing we seem to forget as a profession is the human element. Not just in the success of attack, but perhaps even more ignored, in the success of defense.

The human element in defense

As a field, cybersecurity often focuses on attack as humans applying mechanisms and defense as mechanisms. To the extent that humans are mechanisms of the defense, they are generally studied as weaknesses in the defense, such as their susceptibility to deception and influence operations. But the major human element in defense often ignored or dismissed is the efforts of the human beings who architect, design, implement, operate, maintain, and adapt the defenses.

- Perhaps the reason things are still working is that a lot of hard working, intelligence, serious individuals are paying close attention and applying their knowledge, skills, training, education, and experience (i.e., expertise) to keep things going.

It is this human element in defense that I believe to be the reason we are not all suffering both individually and as a society from the attempts at executing cyber warfare.

The battle is underway

Just as the people of Ukraine are fighting for their lives in a physical battle, many of the people of the world, including those in Ukraine, are also fighting a cyber battle for the future of society.

These people are not in personal physical danger in the same way as the people on the ground being killed every day by the incoming fires from Russia, or the Russian soldiers being killed as the Ukrainians defend themselves. But they are in another kind of danger. This is the emotional danger of exhaustion, feelings of failure, ego and collapse of ego as things go well and poorly, destruction of family relationships from long hours with little emotional support, excessive caffeine, and a lack of professionalism and respect in a workplace that is often out of control.

The battle must be sustained

While the battle in cyberspace can be intense at times, you go back to your house, get a shower, call in a pizza, and so forth. It's not like being in a bombed out building getting shot at. But it's also a lot more complicated than a ground battle from the point of view of the warrior. Simple mistakes can have far-reaching consequences, and real-time work on live systems makes it pretty easy to make a mistake that's hard to recover from.

Burnout is likely to start deprecating the capabilities of the cyber warriors and attrition is likely to become a real issue in a short time frame. Newly trained troops alongside experienced fighters will have to be provisioned, in increasing numbers, and soon. Where is the training ground at high volume? It's in the online environment today, but it needs to be embraced or...

Conclusions

Fear, uncertainty, and doubt again. Sorry about that. The World is not black and white. These issues are complicated and uncertain, and like all issues of war, no plan survives contact with the enemy.[1] I think something we need to understand better is the human element of defense, in the sense of the professional cyber-defender in situations of real-time conflict.

[1] Helmuth von Moltke the Elder - "No plan of operations extends with certainty beyond the first encounter with the enemy's main strength." 1871 per https://quoteinvestigator.com/2021/05/04/no-plan/