Dear Reader,

December 2018

Pulitzer Prize winning historian Henry Adams (1838-1918) observed that politics is “the systematic organization of hatreds.”

This means, among other things, when a high level politician or bureaucrat takes office, he absorbs the geopolitical grudges of his predecessors.

After 68 years, the governments of North Korea and DC still hate each other. After 233 years, Russian leaders and Chechen leaders hate each other too.

For rulers of Japan and China it’s 13 centuries. Since 3600 BC, more than 14,000 wars have erupted.

When Napoleon’s army arrived in Lithuania, he expressed delight at their progress but wrote, “I still don’t know what we are fighting over.”

EWR has warned many times that trade wars tend to morph into shooting wars. As libertarian economist Frederic Bastiat reportedly warned, “when goods do not cross borders, soldiers will.”

On October 4th, Vice President Pence gave a blistering speech against Beijing. His words are widely seen as the declaration of a new Cold War, similar to that of Churchill’s Iron Curtain speech in 1946.

But it came amidst the hate drenched Ford-Kavanaugh battle over innocent-till-proven-guilty vs. guilty-till-proven-innocent. The mainstream news media paid it little attention.

That was irresponsible. Pence’s speech had all the earmarks of a turning point in world history. Here’s the story.

The Cold War between Washington and Moscow was anything but cold. It contained the horrific Korean and Vietnam wars, and the terrifying Cuban Missile Crisis and Yom Kippur War, both of which nearly went nuclear. Also, it gave us a host of smaller, lesser known hate-filled conflicts such as in Cuba, Nicaragua, Guatemala, Afghanistan, Iran, Paraguay, Turkey and elsewhere.

As EWR predicted, escalation of today’s trade war is now intensifying the eyeball-to-eyeball confrontation between Beijing and Washington in the East China Sea and South China Sea. Four days before Pence’s speech, during a game of chicken near the Spratly Islands, a US destroyer and a Chinese destroyer came within 45 yards of crashing into each other.

When it comes to fighting taxes, regulations and the swamp, Trump may be the best leader since England’s 1868 prime minister William Gladstone.

But his insistence that increasing trade barriers will lead to freer trade is, well, do you know of any case in history in which freer trade resulted from more trade restrictions?

I know one, although it worked obliquely. It was the 1930 Smoot-Hawley tariffs. These turned a recession into the Great Depression, creating severe hardship around the world. The poverty brought the meteoric rise of Hitler and WWII.

---

1 A 1984 joint study by research teams at the University of Oslo and Norwegian Academy of Sciences. DIRTY LITTLE SECRETS — MILITARY INFORMATION YOU’RE NOT SUPPOSED TO KNOW, by Dunnigan & Nofi, 1990, p.419.


Ongoing Forecast. The crumbling of the US Empire will last years, and at its most chaotic will have this effect on investments [in terms of today’s dollar]:

<table>
<thead>
<tr>
<th>Investments</th>
<th>Price Now</th>
<th>Highest Price in Today’s $</th>
<th>CL*</th>
</tr>
</thead>
<tbody>
<tr>
<td>Oil (Brent lt. swt. crude)</td>
<td>$70.18</td>
<td>$250</td>
<td>7</td>
</tr>
<tr>
<td>Gold</td>
<td>$1,208</td>
<td>$12,000</td>
<td>8</td>
</tr>
<tr>
<td>Silver</td>
<td>$14.12</td>
<td>$200</td>
<td>8</td>
</tr>
<tr>
<td>Platinum</td>
<td>$858</td>
<td>$12,000</td>
<td>8</td>
</tr>
<tr>
<td>Palladium</td>
<td>$1099</td>
<td>$7,000</td>
<td>7</td>
</tr>
<tr>
<td>Fidelity Defense (FSDAX)</td>
<td>$17.32</td>
<td>$60</td>
<td>9</td>
</tr>
<tr>
<td>PCGS3000 collector coin index</td>
<td>$56,787</td>
<td>$700,000</td>
<td>8</td>
</tr>
<tr>
<td>Rogers Intl. Commodity index</td>
<td>2,409</td>
<td>15,000</td>
<td>7</td>
</tr>
<tr>
<td>S&amp;P/Case-Shiller 20-city resi-</td>
<td>211.67</td>
<td>500</td>
<td>8</td>
</tr>
<tr>
<td>dential real estate index</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

*My present confidence level for this forecast. 10=totally confident. 1=skeptical.

After the war, leaders began to worry that a new era of trade restrictions could trigger another depression and world war.

In 1947, 23 governments began trade negotiations. By 1967, the so-called Kennedy Round, comprised by then of 66 governments, produced one of the greatest eras of freer trade ever. According to economic historian Douglas Irwin, it “helped put the world economy on a sound foundation and thereby improved the livelihood of hundreds of millions of people around the world.”

So, there are two roads that can lead to freer trade. First is the roundabout one created by Smoot and Hawley: trade war, then depression, then shooting war, ending in the Kennedy Round.

Second would be more direct and peaceful. By-pass the trade war, depression and shooting war, and go direct to a new Kennedy Round.

Trump could announce he has decided to skip the long road and take the short one, and call for a new Kennedy Round.

After all, why not? What does he have to lose?

But I think his advisors have done a dreadful job of teaching him economics. When he spoke about Smoot-Hawley on September 30th, he demonstrated a shocking confusion. Did someone purposely mislead him, someone who hates Beijing and wants a war with them?

The beginning of the war may be happening inside your computer right now. Much of this EWR is another update of the internet war resulting from political vendettas all over the world. As we shall see starting on page 3, the cyber war is spreading like kudzu, much faster than I expected earlier in the year.

4 “GATT turns 60,” WALL ST. JRNLS website, Apr. 9, 2007.

It’s affecting practically everything humans do, and invading every corner of your life. I’m not exaggerating, every corner.

As you read, remember, politics, including geopolitics, is about hatreds — deep, dark, despicable ones. My advice: as the cyber war inflames hatreds, watch the South China Sea and East China Sea, and keep a tight grip on your Huntington Ingalls (HII).

We could have no better measure of how much America’s foundations have crumbled than the Kavanaugh debacle. Leaders of the Democratic Party — the traditional 20th century defender of civil rights — came down on the side of the vicious policy of guilty till proven innocent.

A hugely profitable electronic tulip

Publishers and broadcasters do not pay their writers to sit around and not write. The customers want stories, ones that are interesting. Writers are under constant pressure to satisfy this demand. No one wants to buy a newspaper that’s boring.

The publishers, broadcasters and writers all live in fear of “slow news days” in which little happens.

Out of desperation, difficult as this may be to believe, they sometimes turn a molehill into a mountain. Examples are Bigfoot, UFOs, the Flying Dutchman, global cooling in the 1970s, global warming in the 1990s, and climate change today. Each is based on a modicum of facts and a carload of imagination and/or exaggeration.

Occasionally one of these fake mountains is noticed by the financial industry, which is also always under pressure to find something to sell to their customers.

When a slow news day collides with a slow investment day, the result can be a tulipmania. Thousands of investors bid up the price of a fantasy.

In the original tulipmania in the 1630s, some tulip bulbs were sold for 300 gold guilders, about the annual wage of a master craftsman. A few went for as much as 5,000 guilders, the price of a well-appointed house.

If you get into a tulipmania early, you can earn a fortune. But if you come to it late it’s high risk. You must get out before the inevitable crash.

In the Jan. 2014 EWR I suggested speculators get into bitcoins. Those who did and got out early profitted wonderfully. But that mania now is much too long in the tooth for my tastes.

A better bet might be artificial intelligence. Founded as an academic discipline in 1956, AI occasionally experiences waves of interest, and we seem to be entering a new one.

I do not for one minute believe AI is anything more than gonzo number crunching. But in the investment markets, what I think does not matter. What does is what’s in the news — what’s fashionable.

I believe Nvidia (NVDA) is the most promising AI stock. Nvidia is the leading producer of high-speed chips that nearly all AI programs require. I suggested it last year in July, saying I believed it had a 2.5 risk level (on a scale of 1 to 5 with 1 being safest), and a 3-year profit potential of 100%.

That forecast was so far below the mark it almost qualifies as a mistake. Since then Nvidia has been up five-fold.

Nvidia is presently down due to the general market corrections. I consider it a top pick for tulip status, but as such, I’m sticking to the 2.5 risk level.

Another reason I like Nvidia is that for about two decades people have been using the computing tools found on the internet as a substitute for capabilities that once would have been packed into their personal computers. For reasons that will become clear in a few minutes, I think that as the internet grows ever more unreliable, there will be a mania like that of the 1980s and ‘90s, to cram as much computing power into personal computers as possible. Nvidia, with its high capacity chips could benefit wildly.

Lots of other firms are deep into AI. Standout examples are Alphabet/Google (GOOG) and Microsoft (MSFT). But they are also deeply dependent on the internet and, therefore, in my opinion, prohibitively risky.

Pirates, outlaws & investments

In the previous EWR I wrote about the origin and likely thinking of independent military-grade hackers. I may have given the impression that their type of corruption is a recent development.

It’s ancient, part and parcel of the inherent nature of governments. To understand the cyber war that is now affecting us all, we must know a bit about this history.

But before we get into it, let me point out that I’m not a doomsayer. I’m not predicting the end of civilization, or a return to the Stone Age or even the 1950s.

I believe we are returning only to 1995, which was shortly before the internet and smartphones became a global addiction. And, 1995 will be a big improvement over the escalating chaos that’s sneaking up on us now; it’s something to look forward to.

**Like street gangs...**

...governments generally hate each other. Every one is always afraid another will invade its territory and collect the loot.

In the case of street gangs, the loot is the “protection money” paid by businesses and perhaps individuals. If you live on a gang’s turf, the message to you is, pay us a portion of your income or something bad will happen to you.

From governments, it’s the same, but called taxes. If you live on a government’s turf, it’s pay what we demand or something bad will happen to you.

As with street gangs, governments consider their borders to be sacred and they fight wars over them. This requires recruiting soldiers, training, and equipping them.

Some soldiers are employees. Others work more independently, keeping a percentage of the loot they steal.
Visiting the British Army Museum in London many years ago, I saw an amazingly frank exhibit about this. For much of the history of the British Empire, the army was a mafia. Officers had to purchase their commissions. They expected that their troops would steal enough loot to produce a profit.

Much of the vast hoard of art objects in the renowned British Museum and elsewhere was originally property of foreign populations stolen by the British army, carted off to Britain, and split among the honchos:

Incidentally, notice in the glowing TV coverage of the British royal family, no one ever reminds us of where these people got all that wealth.

Such behavior eventually led to the…

...“golden age of piracy”... … which was roughly 1650 to 1735. It sprang from the Hatfields-and-McCoy’s feuds among the governments of Spain, France, Holland and England.

A strategy in these wars was to grant “letters of marque.” These gave permission for armed private ships (“privateers”) to attack and plunder cargo ships and warships of enemy nations.

Often when the war ended and the letter of marque expired, the well-trained and equipped privateers would continue on their own as pirates. Examples are lowlifes such as Francis Drake, Henry Morgan and Blackbeard.

Incidentally, pirates are not the playful characters of amusement park rides and movies. These vermin are avid practitioners of torture, rape, murder and every other kind of brutality. Piracy is the worst possible crime, because it encompasses all others. Not until the 20- century did the entertainment industry begin teaching the young that felonies are good wholesome fun. Wikipedia lists more than 200 pirate films.

This soldier-to-pirate career path... …occurred on land, too. For instance, Jesse James, the Reno Brothers, the Younger Brothers and many other criminals began as soldiers in the Civil War.

Armored with military weapons and trained for military combat, these miscreants found they could do as they pleased, and went wild across the South and Midwest. This brings us back to today.

History is repeating

As explained in the Oct-Nov EWR, the attempt by governments to hurt each other has led them to spend billions of dollars on cyber weapons and cyber training for their hacker troops to damage each other via the internet. These military-trained and equipped troops eventually leave government service, and thousands around the world have become electronic Blackbeards and Jesse Jameses. These pirates roam the internet as wildly as their predecessors did the oceans and countryside.

So, except for being digital, the cyber war — or more accurately, the cyber free-for-all — is nothing new, and it will not end soon. It is a logical consequence of governments hating each other and doing whatever it takes to hurt one another.

Perhaps the most important point to grasp is that the greatest cyber threat is no longer reclusive nerd teen-agers working out of their parent’s basements. It is thousands of electronic Blackbeards and Jesse Jameses trained and equipped for military grade hacking.

These parasites have the tremendous advantage of being on the offense. Offense is easier than defense because the attacker can pick his time and place to strike.

The genius military grade hackers are so adept that expecting any civilian effort to fend them off is like expecting the Chicago police department to defeat the 82- Airborne.

But the young basement pirates are not out of the picture. One thing that makes the super cyber hackers so awful is they create easy-to-use hacking programs and sell them to the basement pirates.

---

Please let that sink in. Weapons of the military rates are being purchased by the hordes of young basement pirates.

On October 9., the GAO (Government Accountability Office) released a report disclosing that the Pentagon’s...

...weapons systems are woefully vulnerable...

...to “increasingly sophisticated cyber threats.” Pentagon officials “believed their systems were secure,” but testing by US military technicians “routinely found mission-critical vulnerabilities,” says the GAO.

The technicians were able to “take control of systems and largely operate undetected.”

Let me emphasize, these were not tests related to personnel records or other low level data. They were tests of the control of “weapons systems.” The report uses the word weapon 282 times.

The GAO cannot legally disclose secret information, but the report contains an illustration that highlights such critical mechanisms as “identify friend or foe systems” and “targeting systems.”

A footnote refers to “a broad range of systems such as aircraft, ships, combat vehicles, radios and satellites” that can be hacked.

The report’s subtitle says the Pentagon is “just beginning to grapple” with the “scale of vulnerabilities.”

So, if even the Pentagon can’t keep itself secure against the thousands of genius cyber hackers, how safe can any business’s or individual’s computers or smartphones be?

Less than a week after my October warning about the cyber war was emailed to you, Facebook disclosed that an attack had released the personal information of 30 million Facebook users.

We are now deep in the global cyber war, and much sooner than I expected. When you are on the internet, you are sailing in a 21st-century version of pirate-infested waters.

So what’s coming?

I can imagine two likely scenarios, which I call earthquake and scorched earth.

You are probably already experiencing the earthquake scenario. Here’s the story.

As things stand now, the collapse of the internet is not coming in a sudden crash and total global paralysis. It’s behaving like an earthquake. An earthquake has foreshocks, a mainshock and aftershocks.

We’re clearly already in the foreshock stage, with incidents of ransomware, viruses, phishing, online scams, Trojan horses, identity theft, emails that disappear or come through altered, children contacted by perverts, and other threats. They’re constant.

Internet-connected household goods are some of the most digitally porous devices — TVs, refrigerators, ovens, coffee pots, dishwashers, dryers and so on. Globally there are already some 10 billion such appliances, few of which have any safeguards. After all, what level of protection should we logically expect in an $18 Wi-Fi-connected lightbulb?

In one case, a casino was hacked through its fish-tank thermometer.8

Reportedly, attacks through such devices are rising at 600% per year. One reason is that many devices are built with off-the-shelf general purpose CPU chips. These can have an array of standard features that the seller does not care about, or even know about, and does not disclose to the buyer.

According to an FBI alert, some internet-connected toys can send a kidnapper or pervert the child’s name, school, likes, dislikes, age, activities, address, conversations, photo and real-time physical location.9

Please read those last five words again. You might also Google “Artificial Intelligence Can Clone Any Voice, Yours Too [Lyrebird].”

The internet reminds me of the old warning from the Vietnam War era: the fact that you’re paranoid doesn’t mean they aren’t out to get you.

Humans are the most adaptable creatures

When things go wrong, they don’t just sit down on the sidewalk, give up and keel over dead. They adapt.

As the foreshocks grow worse, people will increasingly look for ways of getting things done without the internet.

I think foreshocks will gradually worsen in frequency and intensity until one day the world reaches a critical mass of frustration and gives up on the internet. This will be the beginning of the mainshock, in which the entire global internet becomes an electronic ghost town.

My best guess at this time is that...

...we will go through a 3-step adaption

In the foreshock, internet users are making minor adaptions. The mainshock will bring major adaptions, and the aftershock, a plethora of fine tuning.

As a subscriber to EWR, you are much more a forward thinker than most, so you are probably already adapting.

You keep hard copies of everything important to you. You are rigorous about routine backups that are

---


9 FBI Alert number 1-071717(Revised)-PSA
physically separate from the internet and from your computers and smartphones.

Although there is no protection available to civilians that stands much chance against military grade hacking, you have cybersecurity software that protects against low level and mid level attacks.

Therefore, when the mainshock happens, you will already be partly adapted, and so will others.

**Scorched earth refers to...**

...an ancient and common military strategy. It means destroying anything that might be useful to the enemy — food, housing, roads, airstrips, rail lines, water, phone lines, you name it.

Sometimes when a government is losing a battle, it will execute a scorched earth policy not only on the enemy’s population but on its own, to slow the enemy’s advance. Hitler did it to his own Germans, and Stalin to his own Russians.

The October GAO report may someday be seen as the major turning point in the cyber war. Now that the whole planet knows the Pentagon cannot keep its targeting systems from being hacked, every world leader must be in a constant state of anxiety. They know their own computers are probably at least as vulnerable as those of the Pentagon, and no matter how much of their resources they throw at the problem, *they’ll never be confident it has been solved*.

Remember, as explained in the previous EWR, the most effective hacker attacks are false flags:* There is no way to know where they really come from.

Many governments must now be developing what we might call the “final option:” electronic scorched earth procedures.

Think about it. If you were the president of the US or any other nation and were faced with a devastating false flag attack that your cyber defenders could not stop, what would you do?

I think you’d pull the plug. You’d order your people to destroy the entire global internet.

Remember, under a false flag attack, it won’t work for the target to simply cut themselves off from the rest of the world. When they reconnect, the attacker will still be out there waiting to pounce. Very likely, *the only way to get him will be to get everyone*.

The more I think about it, the more I believe this is what’s coming. Some government will find itself helpless to stop a major false flag attack, and will suddenly and without warning go scorched earth, demolishing the entire global internet.

But it won’t be the end of the world. We will not return to the Stone Age. One reason is ...**the attack on Saudi Arabia**

In 2012, Saudi Arabia’s oil industry was hit by the Shamoon “wiper virus” possibly launched by Tehran. Roughly 30,000 computers were infected. Screens went black, files vanished, and email and phones died.

To stop the spread of the virus, technicians had to physically rip out cables and trash computers in Aramco offices around the world.

It was a catastrophe. Replacing it all required an estimated 50,000 new hard drives. Some communications functions came back immediately, but others took as much as six months.

However, the important point for readers of EWR is that *oil production did not stop*. The crude oil, wells, tanks, pipelines, pumps and valves did not vanish. Only the ability to centrally manage them did.

In planning for such an attack, the Saudis had made the production assets independent of the management assets.

It was like the partitioning of modern warships. Damage to a compartment is restricted to that compartment. And, the more compartments, the safer the ship. Like a cork, a warship has so many chambers — anywhere from dozens to hundreds — that the ship can be blown apart, and the pieces will still float. The Saudi network was shattered, but the pieces still worked, although not as efficiently. This brings us to...

**Internet Lite**

We can be sure the IT departments of all large organizations today know about the Shamoon incident and have learned from it. When the mainshock hits, they will likely be at least partly ready, including compartmentization. You will be able to work on your own machine, and perhaps connect with others inside the building, but you will not be able to go outside the building.

Global connectivity will be a memory. The entire planet will be a collection of millions of electronic compartments.

What else will happen? Here are seven forecasts I’m 90% confident about.

(1) As we approach the end of the foreshock period, cybersecurity stocks will soar. For my ten recommendations on these, see the Sept. and Oct.-Nov. EWRs. My guesstimate at this time is that next year will be the beginning of these stocks’ heyday.

---

10 False flag: when an attacker makes the incident look like someone else did it. Often the someone is another of the attacker’s enemies.

(2) As the foreshocks worsen, the whole world population will move to double computers — virgin and non-virgin (see the previous EWR, p. 6). Apple (AAPL) will do wonderfully.

(3) The mainshock will last weeks and in some cases months. The world will instantly regress to something like 1900, as everything that has been made dependent on the internet stops cold. Then, as 1990s kinds of communication and management are reawakened, these facilities will gradually restart.

If in your business or career you are prepared, you will have a big advantage over competitors.

Again, we will not return to the Stone Age. But many born after 1990 will think so. When these people find out they must communicate by moving their vocal chords, and learn if it’s raining by looking out the window, they’ll be outraged. In big cities we could see panic and riots.

You will need emergency supplies such as food, water, medicines and other necessities. They’ve always good to have in case of hurricanes, earthquakes, riots and other disasters too; life is uncertain. See Jim Powell’s Comprehensive Family Survival Guide. The regular price is $97 but I have arranged for my subscribers to get it for just $47. Mention EWR when you call 866-967-4267 or 602-445-2734, or go to www.PowellReport.Com/EWR-FSG

Be sure to have a solar- & crank driven AM-FM radio to receive news of what’s happening. I have not tried it, but the Eton American Red Cross ARCFRX3-WXR Solarlink from Amazon (list price $69.99 + S&H) looks promising.

If your business or job existed before the internet, begin making notes about how things got done then. Store these notes on paper or in your virgin computer; your non-virgin may be killed in the fighting.

(4) In the aftershock period, we will quickly return to an economy something like that of 1995. Computers will be highly capable and running, but connectivity will be degraded 99%, and practically all human activity will be slower than today.

(5) As everyone begins to rediscover the 1995 ways of getting things done, thumb drives and other physical media will become the standard way of transferring data, at 500 mph instead of the speed of light.

In the mainshock, FedEx (FDX) and UPS (UPS) will go through a crash along with the rest of the financial markets, then in the aftershock they will become moon shots.

(6) We will see a run on fax machines.

(7) When the internet returns, big, expensive web sites will have disappeared. They’ll be replaced by small cheap ones that, when attacked, can simply be discarded and reinstated. This will be Internet Lite.

**Internet Armageddon when?**

Impossible to know. The cyber war among governments, coupled with the rogue-hacker free-for-all, has been expanding so fast in recent months that the internet as we know it may not last another two years. Or maybe five. Who knows.

A key point is that the earthquake model is already happening. We are solidly into the foreshock period, and I can see nothing to stop it from evolving into the mainshock.

To me, the biggest mystery is, will the mainshock be a result of a critical mass of people giving up and abandoning the internet? Or will it be from some desperate government going scorched earth?

Consider this: military grade cyber forces are so inexpensive almost any government can afford them. A top quality digital strike force capable of scorched earth can probably be had for less than the price of one B-2 bomber.

Also, there are 206 national governments, plus tens of thousands of regional, state and local ones. Very likely most are already under continual attack by other governments and/or cyber Blackbeards and Jesse Jameses, plus basement nerds.

Therefore, I think there’s a 95% probability the mainshock will be a sudden digital scorched earth.

After all, scorched earth is a typical behavior of governments. Like street gangs with their drive-by shootings that spray whole neighborhoods, in their desire to hurt each other they grow all high and mighty and decide the rest of us are expendable. This political mentality is in the DNA of governments. It goes back thousands of years. It’s what governments do.

**But there’s good news, too**

Once the aftershocks are past and 1995 is here, life will be slower, less stressful and more healthy.

Lots of people who are now slaves to screens, suffering the debilitating effects of 8-hour-per-day immobility, will be driving UPS trucks, flying FedEx planes, and delivering hard copy mail.

The government’s ability to circumvent the Fourth Amendment to spy on us will shrivel.

Shops, malls and Main Streets will revive.

So will privacy, conversation, and politeness.

As screen addiction declines, some people may even begin to notice they have children.

Best of all, “social media” such as Facebook and Instagram will kick the bucket. The skyrocketing suicide rate among teens will dive back to the pre-2007 downward trend, before the advent of smartphones, “likes” and cyber bullying.
In short, we could see a widespread outbreak of sanity and peace of mind.

**What about the cloud?**
I’m a specialist in the behavior of governments, not computers. But I’m sure that the cloud is well-protected against lower and middle grade hacking. The genius military grade hackers may regard the cloud as a wonderful convenience for cyber carpet bombing.

**If your income is dependent on the Internet**
No promises, but if I’m right about today’s internet being wrecked, then think there’s a high probability that late in the foreshock period, if you are in the stocks suggested in previous EWRs, you will earn so much profit you won’t mind.

**Christmas warning**
I wonder how many risky toys and appliances will be given as Christmas gifts this year.

**Please warn those you care about**
The mainstream press is again dropping the ball, paying little attention to the bombshell sneaking up on us. Therefore, I regard this report as another of my most important warnings ever, and hereby give permission for anyone to copy and distribute this EWR as widely as they think necessary.

If you wish to do so electronically, a PDF version is at earlywarningreport.com/Dec2018EWR.pdf

If you are interested in the captivating story of how the feuds among governments turned the internet into a cyber Omaha Beach, get a copy of the new book *THE PERFECT WEAPON* by David E. Sanger.

Sanger explains that cyber offense is “wildly out-pacing defense. … As we put autonomous cars on the road, connectAlexas to our lights and our thermostats, put ill-protected Internet-connected video cameras on our houses, and conduct our financial lives over our cell phones, our vulnerabilities expand exponentially.”

About defenses and weaknesses, he quotes cyber expert Bruce Schneier: “We are getting better. But we are getting worse faster.”

This is not a forecast. The disaster has started.

**I could be wrong about the cyber Catastrophe**
I hope so. But the explosive growth of foreshocks in recent months has made it hard for me to believe the mainshock isn’t coming.

The internet gets my vote as the most poorly thought out experiment ever, and it’s now beginning to fail.

I remember the futurist conference in Aspen, Colorado roughly 25 years ago where I first heard about the internet. Folks around me were excited. But all I could say was something like, *a communications system that will allow every kind of human vermin in the world access to our offices, homes and families? Are you kidding?*

The speaker replied that he was confident someone would solve this problem.

Rarely in history has anyone been so wrong. Maybe an Einstein or Newton will figure out how to stop the spread of military grade hacking. And, maybe he’ll find a way to make governments stop hating each other. But 14,000 wars say this is a bad bet.

If you can find a serious error in this analysis, I’d appreciate hearing from you. Otherwise, I will continue believing we are headed back to 1995, and along the way the investments suggested in the Sept. and Oct.-Nov. EWRs will be spectacular.

Parts of the internet are good. I will continue using them while I can. But I’ll be ready for it all to go belly up at any time.

As additional information about the global cyber crisis — and transition to a calmer, saner, more secure life — comes in, we at EWR will do our best to keep you informed.

Most importantly, I’m fervently looking forward to my loved ones — and you — enjoying a world in which peace of mind is possible.

Happy holidays to you and yours!