Demolición Controlada. Apagones: la siguiente etapa

En este informe se echa un vistazo preliminar a lo que podría ser la próxima gran crisis global, que dejaría a la de 2020, en comparación, como "una pequeña molestia" según afirmó Klaus Schwab.

Por Francis Daimo

1) Consideraciones preliminares

Si se nos hubiera dicho hace un año exactamente por todo lo que íbamos a pasar durante el 2020, seguro nos habríamos reído por lo menos durante un mes seguido, pero no mucho más. Sin embargo fueron muchos los que no fueron para nada tomados por sorpresa por este tipo de acontecimientos, y no me refiero a los participantes de tristemente célebre "Evento 201" sino a varios individuos y colectivos inteligentemente ubicados en distintos puntos estratégicos de todos los mundos visibles e invisibles.

Y si hoy se nos dijera que todo aquello fue solo la primera parte de una suerte de "demolición controlada". ¿Todavía nos reiríamos?

Por más que nos desagrade el hecho, no podemos más que reconocer que aquellos sujetos que ocupan lugares de verdadera dirección (o al menos pueden ser considerados sus portavoces legítimos), son mucho más sinceros que nuestros "líderes" actuales, cuya mejor versión intenta mantener visible la delgada línea que separa "civilización" de "barbarie" y no mucho más. Así como aquellos tuvieron la deferencia de comunicar en tiempo y forma en octubre de 2019 en la Universidad Johns Hopkins [1], hoy (de hecho hace varios meses ya) nos están comunicando del siguiente movimiento de piezas.

Una nueva narrativa se puso en marcha. En pleno verano del hemisferio norte, en el momento en que muchos pudieron quitarse el tapabocas para respirar su cuota anual de oxígeno, la pandilla del Foro Económico Mundial nos estaba alertando de que "habrá otra crisis, será más significativa y debemos comenzar a prepararnos desde ahora" y que "cuando veamos esta nueva crisis esta será más rápida –que lo que hemos visto con COVID– (…) el impacto será mayor y como resultado el impacto económico y social será incluso más significativo".[2] Por su parte, el guionista principal Klaus Schwab [3] está convencido de que "todos sabemos, pero todavía prestamos insuficiente atención, al aterrador escenario de un cyberataque total, que podría traer una completa detención de las fuentes de energía, transporte, servicios hospitalarios…¡nuestra sociedad como un todo!" y pocos segundos después nos da esperanza: "…entonces la crisis del COVID-19 será vista como una pequeña molestia en comparación con un gran cyberataque", por último nos aconseja que utilicemos lo "aprendido" durante la "crisis sanitaria" como una oportunidad para reflexionar sobre el riesgo de una potencial "cyber-pandemia".[4]

Si algo hemos aprendido en el 2020 es que no hay ficción que se atreva a desafiar a la realidad. Aquello que podría ser tomado con liviandad en otro momento de la historia no parece ser un lujo que hoy podamos costear. De haber sido tomado más seriamente el reporte titulado Rebuilding America's Defenses (escrito en setiembre del año 2000), en el marco del Project for the New American Century, probablemente los atentados del 11 de setiembre en la ciudad de Nueva York hubieran sorprendido a muchos menos. [5]

El hecho concreto es que poco después de estas declaraciones-promesas, el Foro Económico Mundial, Derek Manky (el chief of Security Insights, Global Threat Alliances en Fortinet) publica un sugerente artículo en la web del Foro titulado: "Esta es la asociación que precisamos para combatir al cyber-delito global" -("This is the partnership we need to fight global cybercrime") -[6] del 8 de octubre, donde nos recuerda que "igual que la pandemia del COVID, el cyber-delito no respeta fronteras ni ideologías". Algo evidente, si es que esos términos aún tienen sentido. Problemas globales demandan soluciones globales. Siempre existen personalidades dispuestas a promover esta agenda, y el año que recién abandonamos nos dejó sobrados testimonios entusiastas de este ideal regulativo. Las palabras de Manky a este respecto no deben menospreciarse, aún cuando su texto termine con ironías difíciles de digerir: "si algo hemos aprendido del COVID-19 y de los desafíos del distanciamiento social, es el profundo valor de la conexión humana."

2) Razones razonables

Los argumentos principales para justificar los próximos “eventuales” sucesos son plenamente compartibles y de sentido común. Con el aumento exponencial del teletrabajo, un gran porcentaje de la población mundial se vio obligada a mudar su buena parte de su vida al computador de su hogar; sumado esto a la digitalización forzosa de múltiples actividades que hasta hace unos meses no era concebible que fueran accesibles únicamente a través de una plataforma digital (desde la educación formal, pasando por el pago de todas las cuentas pensadas y por pensar, hasta el pedido de frutas y verduras al mercado del barrio). Sin embargo, el “Ciber Polygon Event” [7] (suerte de “Evento 201” pero del 2020) no parece estar abocado a hackeos de tan poca envergadura.

Lo que sigue no es apto para aquellos “teóricos de la casualidad”. Aquellos que sean capaces de ver un patrón en relación a los intereses de las empresas que adhieren al “Ciber Polygon Event” tendrán buenas razones para comenzar a estremecerse. De la misma forma en que la Universidad Johns Hopkins tuvo un papel relevante en establecer las “cifras oficiales” de muertos-COVID (por cuanto los medios masivos de comunicación a nivel mundial se valían de sus números como fuente casi indiscutida),[8] hoy tenemos nuevos socios en la “carrera contra la ciberpandemia” que acecha. En esta oportunidad podemos contar con el “interés” de entidades de la talla de Amazon, Microsoft, Hewlett Packard Enterprise, Hitachi, Huawei, IBM, KPMG, PwC, Dell Technologies y Deloitte. Para aquellos que por casualidad tengan fondos en un banco, tengan la tranquilidad de que el Banco Santander, Bank of America, Itaú Unibanco, JPMorgan Chase, MasterCard, SWIFT9 y PayPal están interesados también. De todas formas, cualquier evento que cuente con el fondo de inversiones más importante del mundo (BlackRock Inc.) y la INTERPOL debería ser una garantía (de algo). [10] Lo que queda claro es el marcado carácter financiero de los involucrados en asuntos de “ciberpandemia”. Es bueno, por otra parte, saber que realmente se tomaron en serio el problema de los potenciales ciberataques que podrían (como pronosticaba un preocupado Schwab) literalmente apagar el mundo. [11]

Lo bueno de estar en 2021 es que para quien lee estas líneas no debería ser un ejercicio tan complejo el visualizar escenarios distópicos y aparentemente inverosímiles. Pido entonces hacer el ejercicio de imaginar un apagón general que dure (al menos) una semana o diez días como máximo. Si se tiene la desgracia de estar en invierno seguramente se sufrirá más, pero el calor no es consuelo cuando las fuentes de energía de emergencia de los hospitales se agoten. Esta imagen de pesadilla parece tan alejada del mundo real si tan solo nuestro mundo real fuera uno que actualmente no es.

Una parte mía no quiere ir tan lejos como para afirmar que está en el guión el dejar sin energía a buena parte del planeta por un tiempo prudencial; aún así, parece haber tanta evidencia como para pensar que algo así no sería del todo descabellado. Además, nuestros medios forjadores de realidad nos lo vienes “avisando” hace meses.[12]

3) Estamos todos conectados

Lo que sigue claramente no es para “teóricos de la casualidad”. No debemos ser tan ingenuos de creer que esto tiene tan solo unos meses de preparación. De hecho, por lo menos desde abril del 2020 que tenemos señales claras en este contexto gracias a la publicación en WEF de Leo Simonovich: “Por qué el COVID-19 está volviendo los servicios públicos más vulnerables a un cyber ataque, y qué se puede hacer al respecto” [13]. Simonovich parece haber encontrado la solución ya para noviembre cuando publicó: “La IA puede proteger a todas las compañías de energía del cyber ataque. Aquí se explica cómo”. [14]

Veamos por ejemplo varias situaciones que se han sucedido desde mediados del 2020 hasta la fecha en relación a los problemas energéticos. Por ejemplo, para fines de octubre de 2020 se reportaba que se estaban evitando “millones de cyber ataques” a la red eléctrica de los Estados Unidos [15], por lo que no sería extraño (ni reprochable) que algún malhechor tuviera éxito. Entiendo que quien se enfrenta a estas líneas desde el sur objete que casi todo el alarmismo se fundamenta en episodios del norte y debo reconocer la parcial racionalidad de dicho planteo. Sin embargo, parece que esos tiempos en que las cosas “pasaban en otro lugar que no es aquí” han terminado. La globalización como un fenómeno que forma parte del zeitgeist hace que tanto los honores como los horrores se manifiesten casi con la misma contundencia en todo el planeta al mismo tiempo. No se me ocurre mejor ejemplo que la crisis de 2020 que no parece haber dejado parcela de tierra indiferente. Por otra parte, haría bien recordar que dos años atrás (en 2019) el Uruguay (conjuntamente con el sur de Brasil y buena parte de Argentina e

incluso Chile) quedaron sin electricidad por varias horas en un evento que nunca tuvo una respuesta clara sobre lo sucedido. Este incidente fue lo suficientemente relevante como para ser cubierto por cadenas internacionales. [16] Por lo que se ve, esta película se proyectará potencialmente también en cines locales.

4) El Plan

Me permito especular en este punto un posible curso de acción para los meses siguientes que no necesariamente tiene que cumplirse en su totalidad. De hecho, esperando que no se cumpla en su totalidad.

El WEF necesita este tipo de situación porque está preparando la siguiente fase de su "Great Reset". Para esto necesita implementar las piedras angulares restantes para la "demolición controlada", un barrido de los gobiernos, fuerzas policiales, poder judicial, sistema bancario, ejército, medios de comunicación y servicios públicos de (por lo menos) los países más influyentes a escala global.

Es por eso que eventualmente se desencadenará una "cyberpandemia" que provocará un apagón en muchos lugares del mundo. Especialmente en Estados Unidos, Alemania, Francia, Reino Unido, Australia y Canadá. En los países del "tercer mundo" esto sería en principio más difícil de lograr porque la infraestructura de servicios públicos no tiene el mismo grado de tecnología, aunque esta situación dista de ser algo homogéneo claramente. Aún así, Internet puede interrumpirse fácilmente en cualquier lugar del planeta, incluso de forma remota (y esto sí que no es algo que últimamente nos pueda sorprender).

Con una "pandemia cibernética", un apagón de Internet y las comunicaciones, es posible poner de rodillas a casi todos los gobiernos, agencias policiales, instituciones financieras y empresas de servicios públicos, de la noche a la mañana en la mayoría de los casos. Ningún gobierno del mundo sobreviviría si no pudiera recuperar la electricidad, Internet y las comunicaciones en cuestión de días. Después de una o dos semanas, países enteros se destruirían a sí mismos desde adentro.

Sin comunicaciones disponibles, los gobiernos y los organismos encargados de hacer cumplir la ley ya no pueden cumplir ninguna función relevante en una sociedad. La gente, que en muchos lugares a esta altura ya perdió todo durante los encierros forzados, comenzaría a tomar las calles. Sistemas políticos enteros y formas de gobierno colapsarían en una semana si un apagón durara el suficiente tiempo. La mayoría, por no decir todos los gobiernos del mundo elegirán las soluciones listas para usar del Foro Económico Mundial, cualesquiera que estas sean para ese momento.

Al momento, este escenario aparentemente de ciencia ficción presenta eventos ciertos que no pueden dejarse de lado con facilidad. Probablemente el apagón en Pakistán [17] así como la amenaza cierta y reciente (27 de enero de 2021) de un apagón masivo en toda Europa [18] sean señales que debemos atender.

5) Conclusiones

Existen razones para estar preocupado, pero más aún para estar ocupado. Nada sería más deseable ahora que poder transmitir un mensaje tranquilizador en cuanto al futuro mediato, pero esto es algo que se hace difícil dada la información que en estas líneas se está haciendo pública.

Si bien es probable (y deseable) que los peores eventos vaticinados no se concreten tal cual fueron previstos, no parecería descabellado tomar medidas acordes a una instancia tal como una pérdida de las fuentes de energía por un tiempo estimado promedio de una semana. Quizás esto nos ayude a valorar qué es lo realmente importante en nuestras vidas (donde seguro no serán las actualizaciones de las redes sociales nuestra primera preocupación).

En definitiva, este Informe pretende poner en la palestra una perspectiva que se entiende atendible y cuyas consideraciones fácticas no son producto de meras especulaciones desprovistas de todo arraigo. Esperemos que lo aquí informado se mantenga en el reino de la conspiranoia.

notas:

1. Dicho Evento tuvo lugar en las instalaciones de la Universidad que poco después sería el referente mundial en el conteo de muertos por-con-de COVID-19 en tiempo real para todo el planeta. Disponible en: https://www.centerforhealthsecurity.org/event201

2. Jeremy Jurgens (Managing Director del World Economic Forum), conferencia del 8 de julio de 2020 en el WEF. Disponible en: https://www.youtube.com/watch?v=msYb8Pk_unk (minutos 57:40 a 1:22:55).

3. Se recomienda enfáticamente la lectura de su libro-manual "COVID-19: The Great Reset" publicado el 25 de setiembre de 2020 en varios idiomas. El mismo está escrito en co-autoría con Thierry Malleret.

4. Klaus Schwab (fundador del World Economic Forum), conferencia del 8 de julio de 2020 en el propio WEF. Disponible en: https://www.youtube.com/watch?v=msYb8Pk_unk (minutos 9:17 a 20:12).

5. Especialmente recomendado es el libro The New Pearl Harbor (2004) de David Ray Griffin para entender mejor todo este punto.

6. https://www.weforum.org/agenda/2020/10/the-partnership-we-need-to-fight-global-cybercrime

7. https://www.weforum.org/projects/cyber-polygon

8. Es sintomático que la primera entrada que Google nos ofrece cuando ponemos en su barra de buscador las palabras "johns hopkins" es el "COVID-19 Map – Johns Hopkins Coronavirus Resource Center": https://coronavirus.jhu.edu/map.html

9. Vale la pena señalar que SWIFT afecta casi sin excepciones las transacciones financieras de carácter internacional.

10. La lista completa de partners se puede encontrar aquí: https://www.weforum.org/platforms/the-centre-for-cybersecurity

11. En este sentido, podemos ver actualizaciones en el blog de Microsoft en diciembre de 2020: https://blogs.microsoft.com/on-the-issues/2020/12/17/cyberattacks-cybersecurity-solarwinds-fireeye donde se menciona como la primera de las tres amenazas principales el continuo aumento en la determinación y sofisticación de los ataques al nivel de los Estados-nación.

12. En octubre el New York Times estaba culpando explícitamente a los rusos de hackear redes eléctricas y plantas nucleares norteamericanas: https://www.nytimes.com/2020/10/23/us/politics/energetic-bear-russian-hackers.html; otros ejemplos de "hackeos" dirigidos específicamente en Estados Unidos a dejar sin electricidad el territorio: https://news.bloomberglaw.com/privacy-and-data-security/hackers-are-targeting-the-remote-workers-who-keep-your-lights-on; los ejemplos abundan desde octubre/noviembre de 2020 e incentivo al lector a realizar su propia investigación. Los ejemplos son tantos que podría ocupar el presente informe con un sumario de los mismos.

13. https://www.weforum.org/agenda/2020/04/why-covid-19-is-making-utilities-more-vulnerable-to-cyberattack-and-what-to-do-about-it

14. https://www.weforum.org/agenda/2020/11/ai-can-protect-firms-from-cyberattacks-during-the-energy-transition

15. https://www.utilitydive.com/news/the-us-power-sector-has-prevented-millions-of-cyberattacks-in-2020-that-t/587949

16. https://www.elplural.com/politica/internacional/un-apagon-deja-sin-luz-a-argentina-y-uruguay-y-partes-de-brasil-y-chile_218654102; https://www.20minutos.es/noticia/3672814/0/apagon-masivo-argentina-uruguay-brasil-chile; https://www.abc.es/internacional/abci-gran-apagon-deja-sin-toda-argentina-y-uruguay-y-partes-brasil-y-chile-201906161416_noticia.html

17. https://indianexpress.com/article/explained/explained-what-led-to-the-nationwide-power-outage-in-pakistan-7140969; https://www.nytimes.com/2021/01/09/world/asia/pakistan-blackout-power-failure.html

18. https://www.bloomberg.com/news/articles/2021-01-27/green-shift-brings-blackout-risk-to-world-s-biggest-power-grid

Referencias

· 20minutos.es. “Un apagón masivo deja sin luz a toda Argentina y Uruguay”. 20Minutos.es. 16 de junio de 2020.
de Carlos, Carmen y Gaviña, Susana. “Un apagón deja a oscuras a gran parte del Cono Sur”. ABC. 16 de junio de 2019.
· El plural.com. “Un apagón deja sin luz a Argentina y Uruguay y partes de Brasil y Chile”. El Plural.com – Periódico Digital Progresista. 16 de junio de 2019.
· Freitas Jr., Gerson y Martin, Christopher. “Hackers Are Targeting the Remote Workers Who Keep Your Lights On”. Bloomberg Law. 30 de julio de 2020.
· Griffin, David Ray. The New Pearl Harbor. 2014.
· Jurgens, Jeremy. “Cyber Polygon 2020”. World Economic Forum’s Centre for Cybersecurity Platform.
· Kuhn, T. y Pizarro, Pedro J. “The US power sector has prevented millions of cyberattacks in 2020 — that takes 24/7 commitment”. Utility Dive. 29 de octubre de 2020.
· Malleret, Thierry. y Schwab, Klaus. COVID-19: The Great Reset. 2020.
· Manky, Derek. “This is the partnership we need to fight global cybercrime”. World Economic Forum. 2020.
· Masood, Salman. “Much of Pakistan Loses Power in Massive Blackout”. The New York Times. 9 de enero de 2021.
· Parkin, Brian; Starn, Jesper y Vilcu, Irina. “The Day Europe’s Power Grid Came Close to a Massive Blackout”. Bloomberg. 27 de enero de 2021.
· Pelroth, Nicole. “Russians Who Pose Election Threat Have Hacked Nuclear Plants and Power Grid”. The New York Times. 23 de octubre de 2020.
· Philipose, Rael. “Explained: What was the cause of Pakistan’s nationwide electricity outage?”. The Indian EXPRESS. 22 de enero de 2021.
· Schwab, Klaus. “Cyber Polygon 2020”. World Economic Forum’s Centre for Cybersecurity Platform.
· Simonovich, Leo. “AI can protect all energy firms from cyberattack. Here’s how”. World Economic Forum. 16 de noviembre de 2020.
· Simonovich, Leo. “Why COVID-19 is making utilities more vulnerable to cyberattack – and what to do about it”. World Economic Forum. 23 de abril de 2020.
· Smith, Brad. “A moment of reckoning: the need for a strong and global cybersecurity response”. Official Microsof Blog. 17 de diciembre de 2020.

fuente: https://extramurosrevista.org/demolicion-controlada-apagones-la-siguiente-etapa/