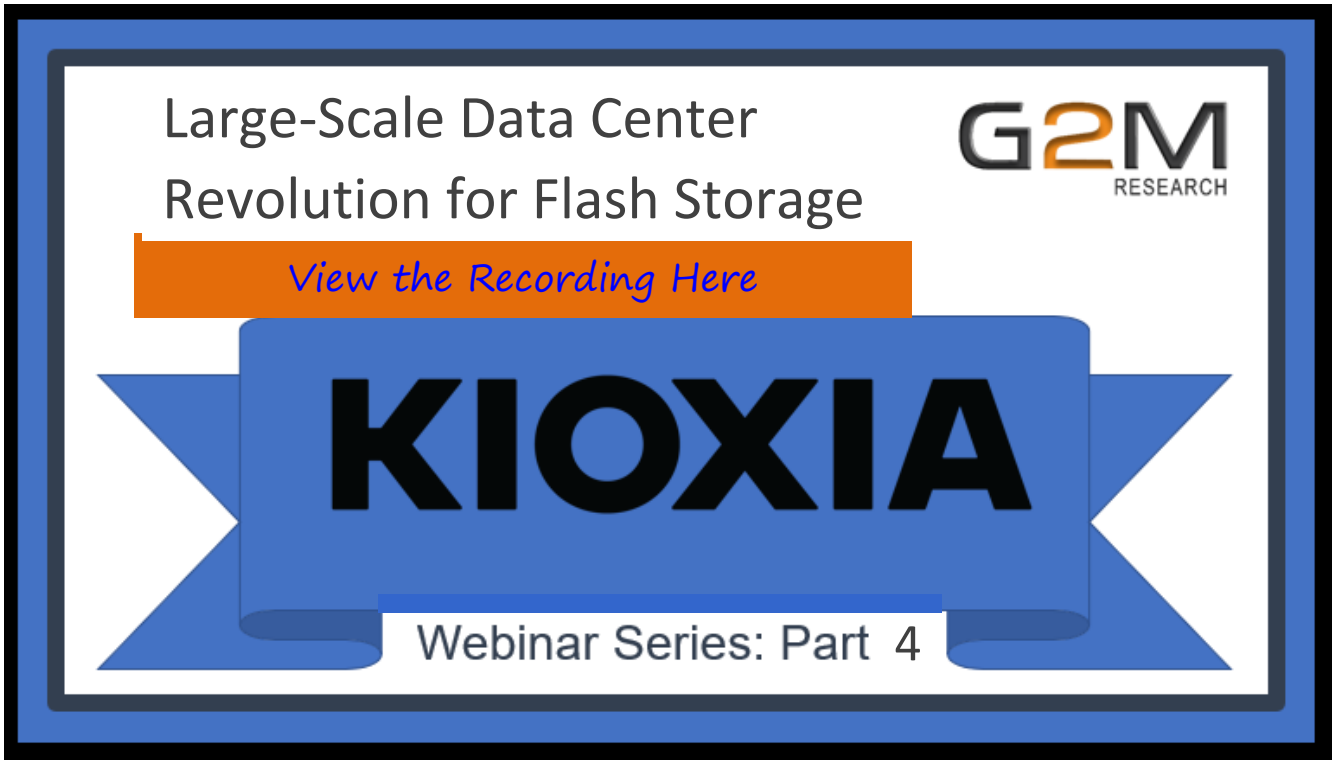
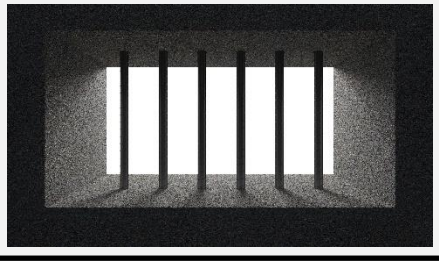
Highlights



"[I]'m not even convinced Russia would know if they decided to take the gloves off, what the genuine impact is. Because so many of the things they may target have fault tolerance, redundancy, can operate off the grid. Being able to do a cyber attack against a utility, and actually shutting it down, are two very different things. And there's a smart precision way to do it. Or there's a blunt force trauma way to do it. So [that said,] here's what's on the menu for Russia. A whole bunch of indiscriminate attacks — just hack and destroy, whatever it is, every industry carte blanche, just hit the button every time you can compromise something, and destroy, destroy, destroy. The impacts of that are almost impossible to guess. And it would just be indiscriminate: all industries targeted. If you can be compromised, you are. If you are already compromised, you are now dealing with encrypted systems or destroyed systems. And we'd be cleaning up on aisle nine all over the place, that's one spectrum. Indiscriminate fraud."

Kevin Mitnick, Security Consultant and Former Hacker, Financial Times, Tech Exchange Interview excerpt

FBI Offers $10M Bounty for Russian Government Employees Indicted in Infrastructure Attacks



The Department of Justice indicted four Russian government employees on cyber crimes committed between 2012 and 2018 targeting thousands of computers, at hundreds of companies, in 135 countries, in a concerted effort to undermine the global energy sector. Akulov, Gladkikh, Tyukov, and Gavriolv attempted to hack oil and gas firms, nuclear power plants, and utility and power transmission companies.

"The potential of cyberattacks to disrupt, if not paralyze, the delivery of critical energy services to hospitals, homes, businesses and other locations essential to sustaining our communities is a reality in today's world," said U.S. Attorney Duston Slinkard for the District of Kansas. "We must acknowledge there are individuals actively seeking to wreak havoc on our nation's vital infrastructure system, and we much remain vigilant in our effort to thwart such attacks. The Department of Justice is committed to the pursuit and prosecution of accused hackers as part of its mission to protect the safety and security of our nation."

None of the defendants are in custody. The U.S. State Department is offering up to $10M for information leading to the arrest of the defendants or the identification of other alleged co-conspirators.

Russian Cyberwarfare: Misinformation & Direct Attacks Against Ukraine

Russian attacks against Ukraine include cyberwarfare measures: 1) Misinformation; 2) Attacks on the IT Infrastructure; 3) Satellite Attacks.

Misinformation

The Security Service of Ukraine destroyed 5 bot farms with a capacity of 100k accounts spreading misinformation and fake news regarding Russia's invasion of Ukraine. The bot farms use social media accounts to distort the news and seek to panic Ukrainian citizens and create chaos and instability. Investigators seized over 100 GSM gateway devices, around 10K SIM cards, laptops, mobile phones, USB drives, and weaponry.

Attacks on the IT Infrastructure

Attacks on the IT infrastructure of Ukraine collapsed connectivity to 13% of pre-war levels but services were swiftly restored. However, the State Service of Special Communication and Information Protection (SSSIP) of Ukraine announced, "In order to preserve its network infrastructure and to continue providing services to Ukraine's Armed Forced and other military formations as well as to the customers, #Ukrtelecom has temporarily limited providing its services to the majority of private users and business-clients." The chairman called these attacks "the first in the human history cyberwar is underway." The SSSCIP said "the entire IT community of the world" is united against Russian and that the hacker community opposing Russia is working to destroy these Russian military cyberwarfare threats.

Satellite attack

A cyberattack targeted a satellite network used by Ukraine's government and military agencies, and knocked thousands of internet users offline, all across Europe including users from Poland to France and access to thousands of wind turbines in central Europe. The attacks crippled modems, then distributed malicious software across the network and overwrote their internal memory. Satellite network owner, Viasat, located in Carlsbad, CA shipped 30k replacement modems to customers in Europe. Viasat enlisted U.S. cybersecurity firm Mandiant to conduct the investigation.

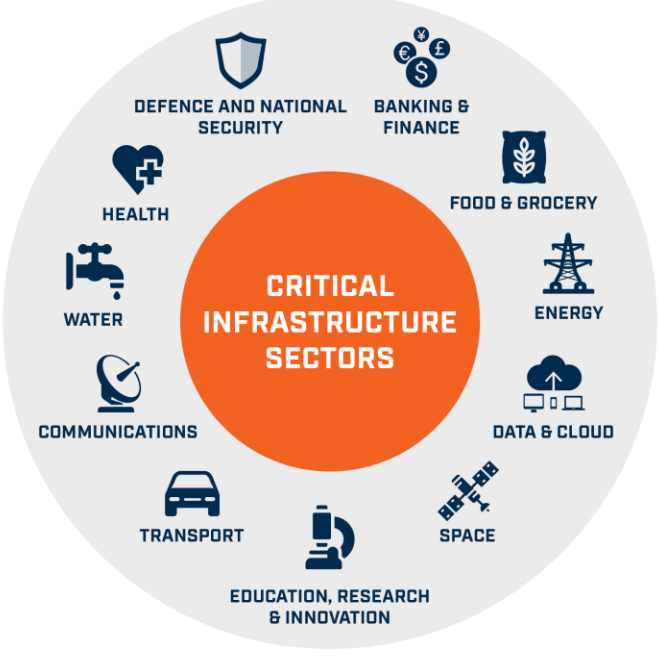
White House Urges Strong Cyber Defense to Protect Critical US Infrastructure

This is a critical moment to accelerate our work to improve domestic cybersecurity and bolster our national resilience. I have previously warned about the potential that Russia could conduct malicious cyber activity against the United States, including as a response to the unprecedented economic costs we've imposed on Russia alongside our allies and partners. It's part of Russia's playbook. Today, my Administration is reiterating those warnings based on evolving intelligence that the Russian Government is exploring options for potential cyberattacks.

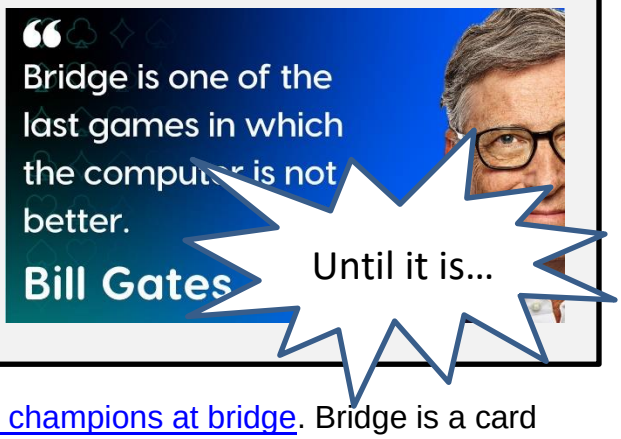
From day one, my Administration has worked to strengthen our national cyber defenses, mandating extensive cybersecurity measures for the Federal Government and those critical infrastructure sectors where we have authority to do so, and creating innovative public-private partnerships and initiatives to enhance cybersecurity across all our critical infrastructure. Congress has partnered with us on these efforts — we appreciate that Members of Congress worked across the aisle to require companies to report cyber incidents to the United States Government.

My Administration will continue to use every tool to deter, disrupt, and if necessary, respond to cyberattacks against critical infrastructure. But the Federal Government can't defend against this threat alone. Most of America's critical infrastructure is owned and operated by the private sector and critical infrastructure owners and operators must accelerate efforts to lock their digital doors. The Department of Homeland Security's Cybersecurity and Infrastructure Security Agency (CISA) has been actively working with organizations across critical infrastructure to rapidly share information and mitigation guidance to help protect their systems and networks

If you have not already done so, I urge our private sector partners to harden your cyber defenses immediately by implementing the best practices we have developed together over the last year. You have the power, the capacity, and the responsibility to strengthen the cybersecurity and resilience of the critical services and technologies on which Americans rely. We need everyone to do their part to meet one of the defining threats of our time — your vigilance and urgency today can prevent or mitigate attacks tomorrow.



Bridge Requires More Human Skills Than Other Strategy Games, Yet AI Is Victorious



In a remarkable victory, AI NooK defeated eight world champions at bridge. Bridge is a card game that includes reacting to the behavior of other players and relies on communication between partners. The two day challenge included 800 consecutive deals divided into 80 sets of 10. Each champion played their own and their dummy partner's cards against a part of opponents. NukkAI, NooK, won 83% of the sets.

Jean-Baptiste Fantum, co-founder of NukkAI said the company has been developing NooK for the last five years and, while confident that NooK would be victorious in thousands of deals, he was not as confident about winning with only 800.

Explainability is a key aspect of the game and is a hot topic in AI. NooK represents a neurosymbolic approach to learning. "Rather than learning by playing billions of rounds of a game, it first learns the game's rules and then improves its play through practice. It is a hybrid of rules-based and deep learning systems" – an approach that more closely mimics human learning.

World bridge champion Nevena Senior said the contracts the champions and NooK were given to play were sufficiently variable and she found that it read opponents better than humans did, "and was better able to exploit their mistakes." "This is something that humans do after enough experience and I was pleasantly surprised that a robot mimics typical human skills."

1996	IBM Deep Blue chess machine wins a game against world chess champion Garry Kasparov but loses the match 2-4.
1997	Deep Blue wins the rematch
2007	Researchers build a checkers-playing computer that cannot be beat.
2011	IBM Watson defeats Jeopardy champions Brad Rutter and Ken Jennings for $1M
2016	Google DeepMind AlphaGo beams Korean Go champion Lee Sodel 4-1 and is awarded the highest Go grandmaster rank, an honorary 9 dan.
2022	NukkAI Nook defeats eight world bridge champions in Paris

"I see AI and machine learning as augmenting human cognition a la Douglas Engelbart. There will be abuses and bugs, some harmful, so we need to be thoughtful about how these technologies are implemented and used, but, on the whole, I see these as constructive."

Vint Cerf, Chief Internet Evangelist, Google

Polls Results for Large-Scale Data Center Revolution for Flash Storage KIOXIA

What is the biggest problem in your datacenter when deploying flash storage at scale (select one)?

"Noisy Neighbors":	7%
Different quality of service/SLA requirements across apps:	7%
Migrating from one flash media to another:	29%
Managing data placement across flash devices:	**36%**
Other issues:	21%
None of the above:	0%

Do you have any projects where software-enabled flash could provide value underway or in planning (select one)?

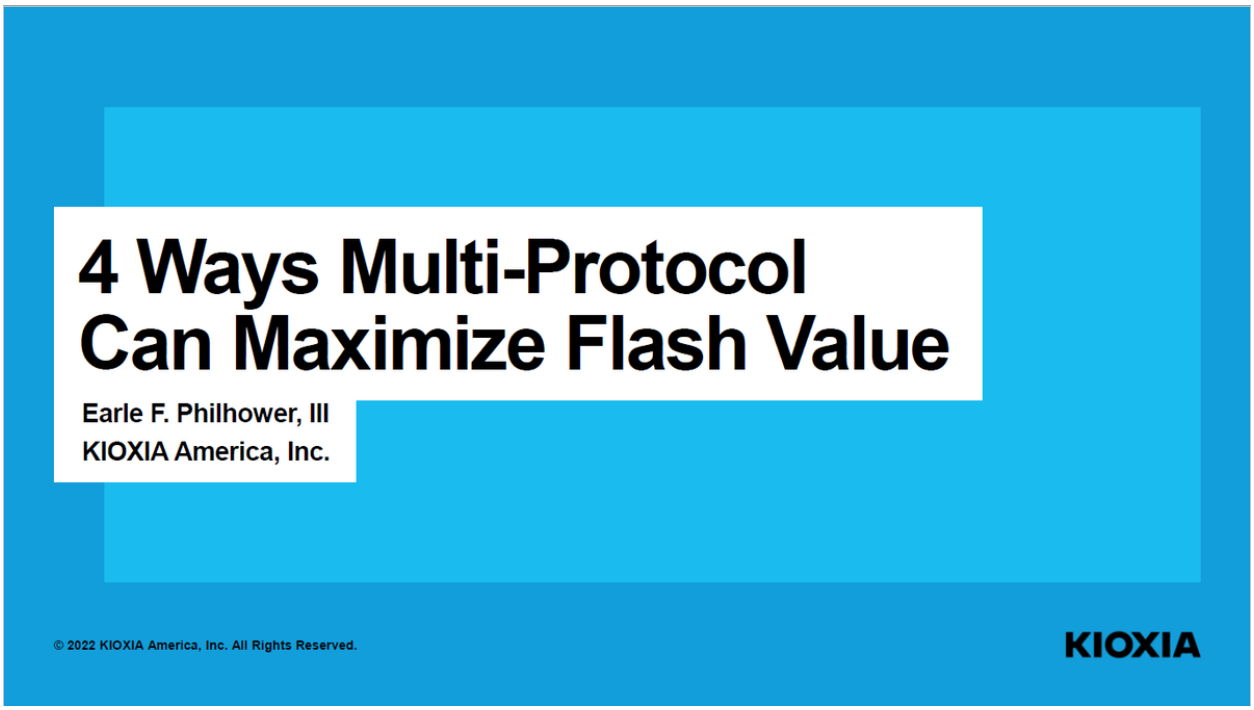
We are currently deploying flash storage for a project where SEF would definitely be of value:	7%
We are planning a flash project where SEF would definitely be of value:	13%
We are planning a flash project where SEF could have some value:	13%
We do not have any projects where SEF could have significant value:	7%
No opinion:	60%

KIOXIA Webinar Series

Wednesday, March 30, KIOXIA presented “Large-Scale Data Center Revolution for Flash Storage.” Large-scale data centers present unique challenges for the optimal use of flash storage. Problems such as "noisy neighbors", data placement, and the widely varying latency requirements of different classes of applications are incredibly difficult to solve simultaneously with conventional flash architectures. Software-enabled flash (SEF) provides a means to effectively address the challenges of cloud data center. Find out how KIOXIA is approaching these issues with its market-leading approach to SEF by viewing the webinar here and the slidedeck is available here.

Tuesday, February 8, KIOXIA provided an analysis of “4 Ways Multi-Protocol Can Maximize Flash Value.” The webinar video is available to view here and the slidedeck is available here.
Each webinar stands alone and collectively provides an overview of the innovation, direction, and leadership KIOXIA provides in this enterprise storage space.

November 17, KIOXIA presented the second webinar in their four-part webinar series, “The Next Flash Revolution at Scale: Open Source Software + Software-Enabled Technology.” The video is available to view and a copy of the slidedeck is available here. KIOXIA webinar Part 1, “Why Flash Memory At Scale Should be Software-Defined” is available to view here along a copy of the slidedeck here.



Upcoming Conferences

April 19-21	ODSC East, Boston
April 23-27	NAB, Vegas
April 26-28	Smart NICs Summit, San Jose
May 4-5	World Summit AI Americas, Montreal
May 9-11	Gartner Data & Analytics Summit, London
May 10-13	Black Hat Asia, Singapore
May 11-12	AI & Big Data Expo, Santa Clara
May 11-12	Cyber Security & Cloud Congress, Santa Clara
May 18-19	Gartner Digital Workplace Summit, London
June 6-9	RSA Conference, San Francisco & Virtual
June 7-10	Women in Tech Global Conference 2022, TBA & Virtual
June 12-16	Cisco Live, Vegas
June 14-16	Digital Enterprise Show, Malaga
June 15	Cloud Security Summit, Virtual
June 21-22	Gartner Security & Risk Management Summit, Sydney
June 21-22	Gartner Digital Workplace Summit, San Diego
June 29- July1	Mobile World Congress, Shanghai
July 19-20	Cyber Solutions Summit & Expo, Virtual

August 2-4	Flash Memory Summit, Santa Clara
August 6-11	Black Hat USA, Vegas
August 11-14	DEF CON 30, Vegas
September 13-14	CISO Forum, Virtual
September 19-20	Industry of Things World, Berlin
September 28-29	IoT World, Santa Clara
October 5-6	Evolve, Vegas
October 24-27	ICS Cybersecurity Conference, Hybrid/Virtual
November 16	San Diego Cybersecurity Conference, Hybrid
November 16	Threat Hunting Summit, Virtual
November 18-19	Data Strategy & Insights (Forrester Research), Virtual
December 1-2	AI & Big Data Expo Global, London
December 6	Security Operations Summit, Virtual