Christian Science Monitor reporting: The Ukranian city of Odessa is said to be home to the world's largest online stolen credit card data marketplace, and the country at large rivals Russia in the pantheon of cyber-crime. Indeed, Ukraine has become a magnet for Russian hackers gravitating to the digital crime syndicates there.

Now, a beleaguered and indebted Ukraine is asking for help from the International Monetary Fund, which gets 17 percent of its money from the US. For Sens. Mark Warner (D) of Virginia and Mark Kirk(R) of Illinois, this presents an opportunity.

"Ukraine is a known hub for cybercrime, and the United States should work with the Ukrainian government to create a framework of cooperation to deter, prevent and counter these cyber criminals and ensure the safety of the newly formed Ukrainian government and financial system," said Senator Kirk in a statement.

Ukraine-based cyber-criminals have become notorious internationally. One big seller of the credit- and debit-card information stolen in the hack on Target stores lives in Odessa.

"A network of underground cybercrime shops … all traced back to a miscreant who uses the nickname Rescator," said Mr. Krebs in a Jan. 14 blog post. "Clues about Rescator's real-life identity suggested he might be a particular young man in Odessa, Ukraine."

An even more intriguing Ukrainian cyber-crime operation involved IMU, which appeared to be a legitimate company incorporated in Belize but with main offices in Ukraine's capital, Kiev. IMU appeared to employ more than 600 employees in Kiev, with subsidiaries in India, Poland, Canada, and the US, according to McAfee, a cyber-security firm. It posted job offerings including receptionists, financial managers, webmasters, and R&D engineers.

But IMU's primary product was "scareware," which infects computers and makes a bogus message pop up on the screen, saying the machine is infected with a destructive virus. It tells the user to call IMU, which will fix the problem. Once IMU has its money, it turns off the bogus pop-up.

IMU responded to about 2 million calls in 2008, according to Nir Kshetri, professor of management at University of North Carolina at Greensboro, in a recent report on Eastern European cyber-crime.

A 2010 federal indictment said IMU cost Internet users in 60-plus countries more than $100 million. The FBI says the company now appears to be defunct.

The Senate legislation unveiled Monday would create a law enforcement partnership between the United States and Ukraine to combat cyber-crime and improve cyber-security. It also recommends that the US develop an extradition treaty with Ukraine, suggesting the lack of one is an important reason why Ukraine has become a haven for cyber-criminals.

Cyber-crime is among the top five most common economic crimes in Ukraine, according to a 2012 study by Ryerson University in Toronto. But for much of the past decade, Ukraine’s record in bringing cyber-criminals to justice has been poor.

Of the roughly 400 people arrested in the country on Internet and banking fraud charges from 2002 to 2011, only eight were convicted, according to Dr. Kshetri’s report.

Some progress has been made since 2009, when the FBI stationed a supervisory special agent at the US Embassy in Kiev to assist with cyber-crime targeting the US, the report adds. And Ukraine has also devoted more resources to its computer crime and fraud enforcement in recent years, Kshetri says in an interview.

Last June, Ukraine’s cyber-security agency, known as the SBU, announced that it had broken a cyber-crime ring that stole $72 million using the Conficker botnet, a piece of malware that began infecting computers around 2008.

But Kshetri suggests there is a long way to go. “Corruption has enabled and generally encouraged [cyber-criminals] to obtain the right to reside and operate criminal activities in the country,” he says in his study. “The IMU case provides evidence to support this hypothesis.”