GERMANS DETECT HAND OF RUSSIA AS POLITICAL CYBER WAR ESCALATES

- 30.12.2016

Financial Times, 29 Dec 2016

I knew this could be possible, says the longest-serving member of the parliaments intelligence control committee. But that it hit the Bundestag was a surprise. I looked again at my communications. I became even more careful with my mobile phone.

If the initial attack on parliaments lower house sent shockwaves through the German political and intelligence establishment, it has since become apparent that its implications could be far worse.

Claims from the CIA, the US intelligence agency, that it has high confidence Russian hackers tried to influence the US election in favour of Donald Trump have boosted fears that Moscow is targeting next years German polls, when Chancellor Angela Merkel is standing for re-election.

German security officials have said last years assault on the Bundestags computer network was also carried out by Russia-backed hackers seeking ammunition for electoral meddling. Earlier this month, Ms Merkel warned that there were signs of internet-based attacks and misinformation campaigns coming from Russia that could play a role in the election campaign.

The government has reacted to the Bundestag attack with a complete overhaul of the parliaments computer systems. But it is also throwing its weight into increasing defences against cyber warfare more broadly, in response to a rising numbers of attacks and the threat of escalation such as the possible sabotage of government institutions and utilities such as power plants. The defence ministry has stepped up its electronic warfare capabilities with the creation of a new 13,500-strong cyber unit, due to be fully operational by mid-2017.

Berlins concerns are shared with other EU states, notably France, which holds a presidential election next year. EU officials fear Europe could be more vulnerable to interference than the US because of its wider political and economic connections to Russia, significant Russian-speaking minorities in some countries including Germany and President Vladimir Putins support for rightwing populist parties across Europe.

Stefan Meister, a Russia expert at the German Council for Foreign Relations, says that as in the US, cyber attacks could be combined with social media manipulation and political support for the Russia-friendly populist and Eurosceptic Alternative for Germany party.

Russian interference in German politics has already started, says Mr Meister. Every country has the right to promote its interests in another country. But Russia has a programme that includes grey tactics and illegal tactics.

The federal Verfassungsschutz, Germanys domestic intelligence agency, has accused Russian

secret services of backing the hackers responsible for the Bundestag attack. The agency blames the breach on a group of hackers known as APT 28, which European and US intelligence officials regard as Moscow-backed. US officials have said the same group, and a related one called APT 29, hacked the Democratic campaign offices ahead of the US presidential election and copied thousands of files. These included emails from Hillary Clinton, the defeated Democratic candidate, which were later also published on WikiLeaks.

WikiLeaks also recently published sensitive German government documents on US-German intelligence co-operation, which officials fear may have come from the Bundestag hack.

It is Russias intention to destabilise the German government and so weaken our democracy
The interior ministry says Germany needs resilient computer systems to withstand attacks, effective intelligence work and citizens that are aware of the potential dangers, including the risk that stolen information could be used to influence opinion. But there is wide concern that the population remains insufficiently prepared.

Mr Ströbele, an opposition Green MP, says he has increased his own security, including using encrypted links for sensitive phone calls. The precaution only works if the person on the other side of the call does the same however. Colleagues have also taken precautions. But not enough in my view, he says.

Thomas de Maizière, interior minister, has warned Germany must be ready for attacks from all sources, including private organisations and criminal groups as well as states such as Russia and China.

Last month, for example, an assault on Deutsche Telekom caused network problems for 900,000 customers, with officials citing criminals among potential suspects. ThyssenKrupp, the steelmaker, which disclosed this month that hackers who stole sensitive data were likely to have been based in Southeast Asia, said bluntly: It is currently virtually impossible to provide viable protection against organised, highly professional, hacking attacks.

Mr Ströbele, who takes a critical view of western as well as non-western intelligence activities, argues that US as well as Chinese and Russian hackers pose a risk to Germany. But government officials say the threat from Russia is of a different order because of its suspected state backing, sophisticated interaction with the media and social media and apparent clear political purpose.

Stephan Mayer, the parliamentary interior affairs spokesman for Ms Merkels ruling CDU/CSU bloc, sums up the fears, warning: It is Russias intention to destabilise the German government and so weaken our democracy.

Cyber attacks, including the kind that in Russian doctrine are called hybrid warfare, now belong to normal daily life, warns Ms Merkel herself, adding: We must learn to manage this.

Kaynak/Source: