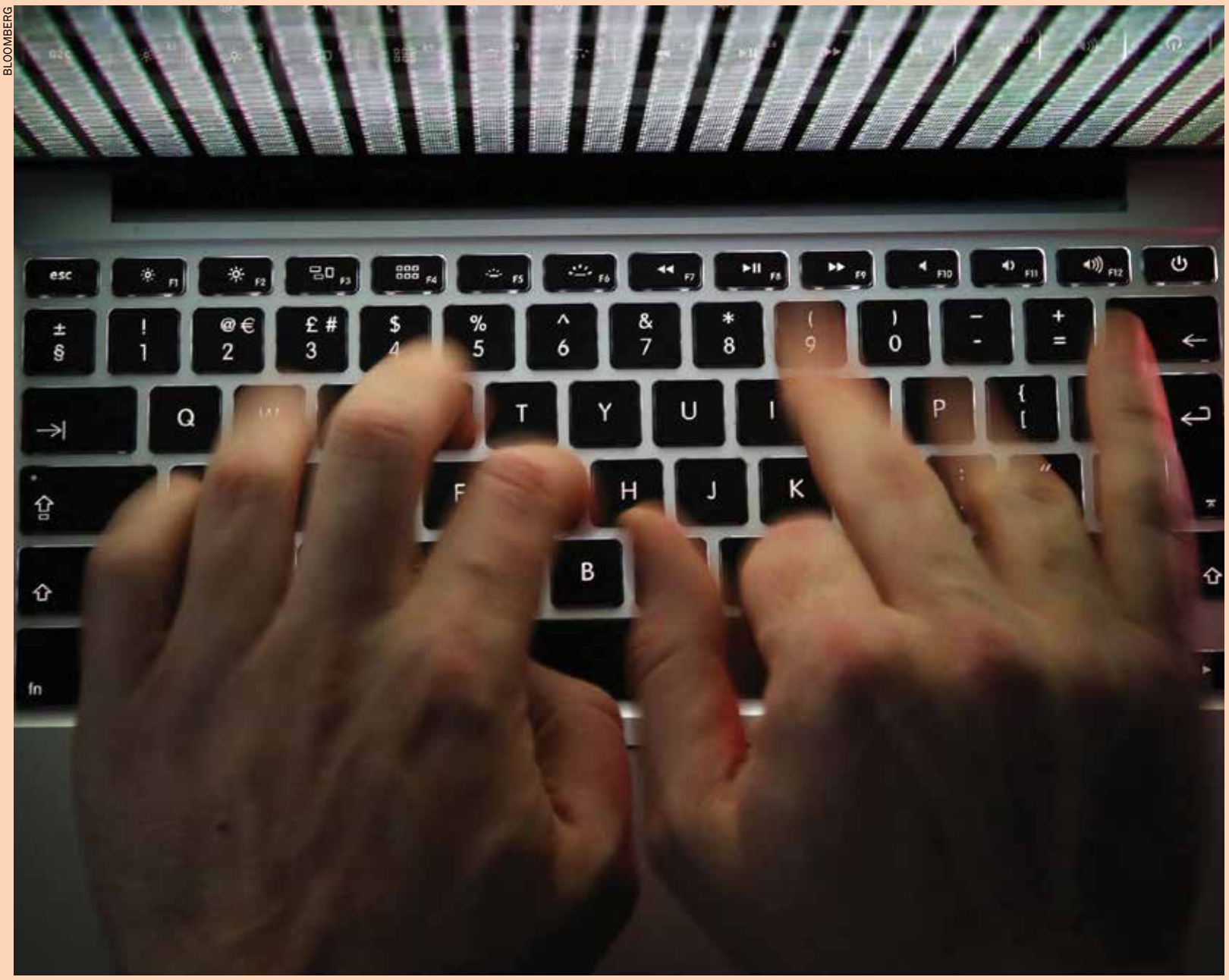
Syndicated articles from
FINANCIAL TIMES
In partnership with
MacauDaily 澳門每日時報 Times

Edition 2751 FT | 27 Feb 2017

Russia's cyber warriors

BLOOMBERG



By Sam Jones

It was an early dinner by Parisian standards, 8.40 p.m., on a mild spring evening at Prunier, an opulent seafood restaurant near the Arc de Triomphe. Amid the hum of conversation, the cracking of shellfish and the gentle chinking of glasses, Yves Bigot missed the insistent ringing. "Then I saw - multiple missed calls, SMS messages, emails, the whole shebang," he recalls. "Both my phones were going berserk."

Frantic staff at TV5Monde's nearby offices had been trying to get in touch with their boss. Something had gone terribly wrong.

It was April 9, 2015, and the channels across TV5Monde's network, the world's largest francophone broadcaster, began switching off, one by one. Hundreds of television screens at its headquarters, from the lobby to its broadcast galleries, had fallen silent. In its basement, the TV network's servers were being systematically erased, digital piece by digital piece.

As he scrolled through panicked emails, Mr Bigot, the broadcaster's director-general, opened a picture message on his phone. A colleague had taken screengrabs from the channel's website and social media accounts: in place of the usual turquoise signage was the shahada - the Muslim profession of faith - written in white on black. Above it: "CyberCaliphate. Je suIS IS".

> **APT 28 has been active for at least a decade, hitting some of the most sensitive military and diplomatic organisations in the West**

Surrounded by squads of heavily armed counterterror police, a team of engineers worked through the night to save the network. They did so by a hair's breadth.

In the days that followed the expected claim from ISIS, of responsibility for the attack, never arrived. Cyber intelligence agents were on site for weeks conducting a forensic search to identify the culprits. Two months later, ANSSI, France's cyber security agency, briefed Mr Bigot. The attack had not been the work of the Islamist group at all. Instead they believed responsibility lay with a group known as APT 28. They were Russian.

A year later, in the spring of 2016 during the US election campaign, APT 28 would initiate an even more audacious operation. The group hacked the Democratic National Committee, releasing thousands of files to discredit Hillary Clinton and calling into question the sanctity of the US democratic system.

The scale of the attack shocked the US, if not the entire western security community. But for those familiar with APT 28's evolution, and the shift in its operations represented by the attack on TV5Monde, it came as no surprise.

"The curtain is still being pulled back," says Shawn Henry, a former assistant director of the Federal Bureau of Investigation, now president of CrowdStrike, the cyber security company drafted in to defend the DNC. "People still don't understand the implications and the impact of these types of attack […] We're further away from [security in cyber space], in the US, than we were eight years ago."

The Financial Times has spoken to more than a dozen leading professionals with close knowledge of APT 28's activities - including senior intelligence and military officials, as well as civilian cyber security experts who have first-hand experience of the group's hacks.

Officials in the US, UK, Israel and Germany have all told the FT that they believe APT 28 is run by Russia's sprawling military intelligence arm, the GRU. Moscow has consistently denied any connection to APT 28.

Many agencies fear the group's activities are far from over. Cyber attacks on NATO are up 60 percent in the past year, according to one official at the alliance. Attacks against EU institutions are up 20 percent, says one senior security source at the commission.

The trail of evidence left by these attacks, while far from comprehensive, goes some way toward indicating the way Russia under President Vladimir Putin sees the world, and how the modern Russian state must secure its place within it. It is one of tactical opportunism and flexibility, but also deep and considered strategic commitments, lines of attack and influence, that have been years in development.

APT 28 has already compromised the computers of political parties in both France and Germany, which have national elections this year, says one senior industry analyst who declined to be named. Since the DNC hack, it has initiated "several" significant new operations, he adds. And hacked dozens of non-governmental organisations targeting most of the aid organisations working in Syria, including those providing information about casualties, according to a western security official.

"Putin and his team are the heirs of the Tsarist, and particularly the Communist secret services," says Chris Donnelly, founder of the Institute for Statecraft and former adviser to successive NATO secretaries-general. "Their understanding is one of permanent conflict with the west in which information has always been a very important issue. Influence and subversion and the whole issue of what they call active measures, or dirty tricks, anything short of declared war, is there to be run."

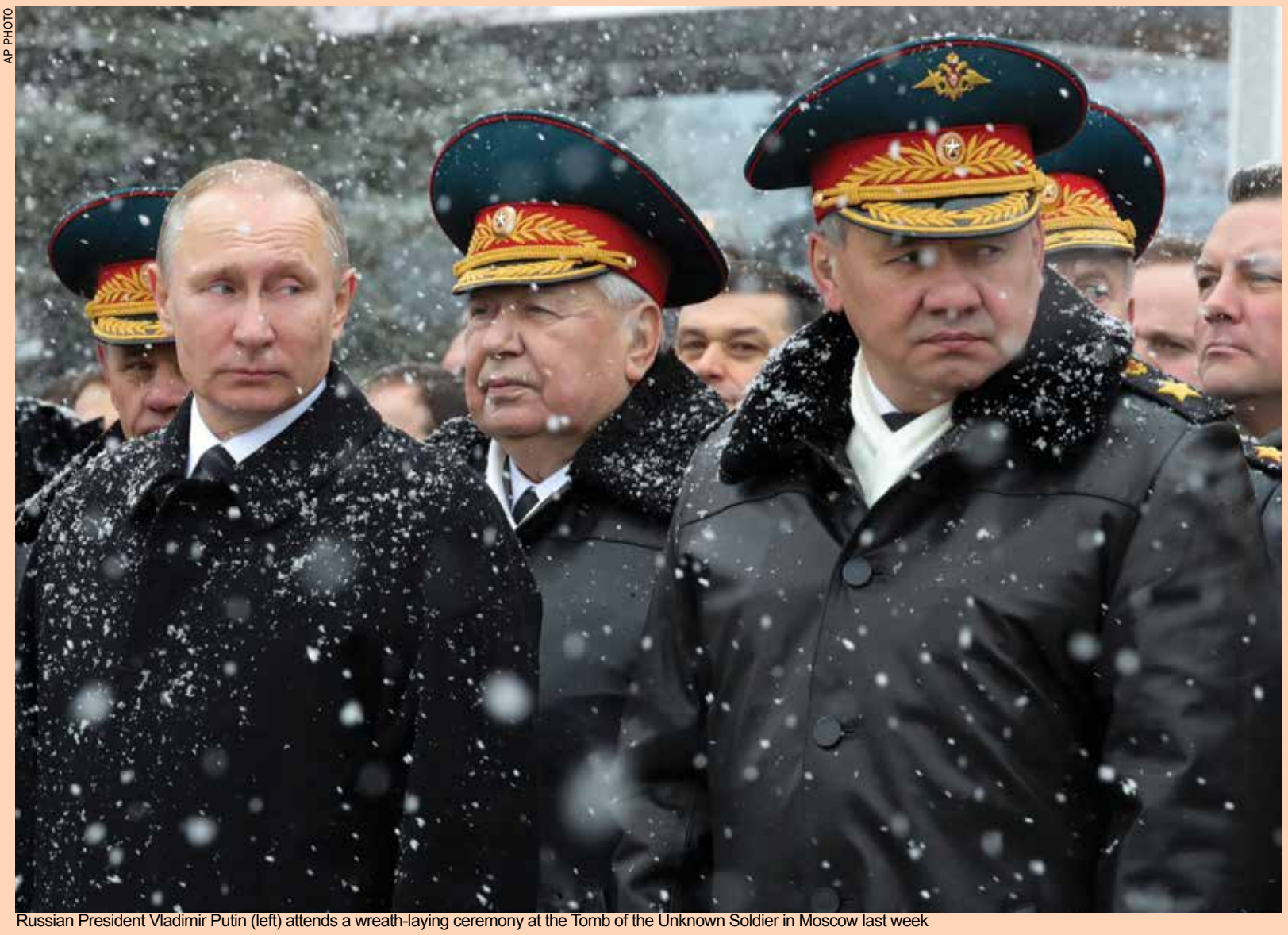
A forensic analysis of high-profile hacks suggests APT 28 has been active for at least a decade, hitting some of the most sensitive military and diplomatic organisations in the west. According to cyber security analysts, previous targets have included Academi, the private military company formerly known as Blackwater; US defence and intelligence contractor SAIC; the French and Hungarian defence ministries; NATO military attaches; the Organisation for Security and Co-operation in Europe; and the US State Department.

Its coding and technical capability is "top level", says one British security official. But more distinctive is the group's mastery of phishing attacks - sophisticated fake emails with realistic, but infected attachments. The FT was shown samples of some of the lures used by the group. In 2010, for example, NATO military attaches in Ankara were sent emails purporting to be from colleagues, with Excel files attached containing a list of their NATO peers' contact details. The trick proved effective and was repeated two years later when APT 28 sent a tweaked version - a list of contact details for senior Brit-

Syndicated articles from
F2 FINANCIAL TIMES
27.02.2017
Macau Daily Times

Russia's cyber warriors (continued)

AP PHOTO



Russian President Vladimir Putin (left) attends a wreath-laying ceremony at the Tomb of the Unknown Soldier in Moscow last week

ish military figures - to embassies across London.

By opening the files, recipients would unwittingly install APT 28's malware on to their computers. From those initial small digital bridgeheads, the group spread its surveillance tools across target networks, often giving it access to classified material and opportunities to cause immense damage.

Costin Raiu, head of global research at Moscow-based cyber security firm Kaspersky Labs, says APT 28's resources distinguish it from other hacking groups. What sets it apart, Mr Raiu says, is the number of "zero day" attacks - operations which exploit flaws in software unknown to the manufacturer - that it carries out at a cost to the group of well over USD100,000 a time. In 2015, the group carried out six known zero-day attacks.

The group's activities can be traced back to 2007 by analysing the code in its malware but it was not until 2014 that the scale of its work became too difficult to disguise. "[That] was when we got our first real foothold on the infrastructure this group was operating," says Laura Galante, director of global intelligence at FireEye. By taking samples of the hackers' malware, essentially their digital fingerprints, the cyber security group compiled a history of the group's activities. It was FireEye that first dubbed the group APT - advanced persistent threat - 28 in a 2014 report.

Other cyber security and tech companies have conjured even more elaborate monikers for the group: Sofacy, Strontium and Fancy Bear among them.

"Russia spends USD300 million annually on its "cyber army" of about 1,000 people

The evidence, collected from hundreds of historical incidents involving APT 28, points towards Russia.

"There is a decade-old professional effort behind this, with at least two different sets of minds in the operation. One a tool development effort and one researching what the targets look like and orchestrating the operations," says Ms Galante, adding that it has all the hallmarks of classic spycraft.

French intelligence agencies that investigated the TV5Monde case have stopped short of drawing a firm line between the group and the Kremlin.

Regardless the ANSSI concluded that the TV5Monde assault was a work of considerable sophistication. Beginning in January 2015, just days after the attack on the Paris office of the satirical magazine Charlie Hebdo, APT 28 mapped out the interlocking computer networks and broadcasting hardware that formed the backbone of TV5Monde's systems. The endeavour would have required telecommunications engineers, skilled coders and, to plan and execute it, tacticians. There were at least seven different "vectors" of entry, ANSSI found.

The attack was only thwarted by luck. TV5Monde had 10 IT specialists working that evening instead of the usual two because of the launch of a new channel earlier that day. It was one of the extras who identified the internal server APT 28 was using to orchestrate its rampage. He ran down to the basement and yanked its cabling out of the sockets. "He's kind of a hero here," says Mr Bigot.

The crucial question, though, is why APT 28 shifted from years of covert intelligence gathering to a riskier operation of aggression, sabotage and manipulation. The attack on TV5Monde, says Mr Bigot, "was like a demo tape."

Kremlinologists and the western intelligence community are still divided on the timing of Russia's altered course in relations with the west: some date it to Kiev's Maidan revolution in 2014 and subsequent invasion of eastern Ukraine; some see a slower-burning breakdown, with Moscow's paranoia exacerbated by years of freewheeling US foreign policy and enthusiasm for regime change; a smaller group see an ever wider arc in which Russia is reasserting its Soviet, even Tsarist, geopolitical behaviour.

Russia's military does not tend to talk of cyber warfare, as the west does, in tightly proscribed, legally measured actions, but rather discusses the broader concept of an information war, a concept that precedes the Soviet era, in which the toolkit has been brought up to speed for the digital era.

Last week, Russian defence minister Sergei Shoigu confirmed the existence of "information troops", rumoured for years but long denied by officials. "Propaganda must be smart, literate and effective," he told the lower house of parliament. Russia spends $300 million annually on its "cyber army" of about 1,000 people, according to the Kommersant business newspaper.

Andrei Soldatov, co-author of The Red Web, says the Kremlin has long seen cyber security as part of a broader concept of information warfare. "They really believe they are under some sort of siege," Mr Soldatov says. "They believe that they lost the first Chechen war thanks to journalists, so when they are in a crisis, the first thing they need to do is control the information space."

Russia analysts say there is a structural dynamic to the rise in APT 28's activity. In 2013, Mr Putin ordered a modernisation of the way Russia controls its operations abroad. It created the National Defence Control Centre, designed to co-ordinate everything from propaganda, economic influence and intelligence through to conventional military operations.

"When they are looking at all these forms of conflict and competition now, they do so with a unified coherent view of how they should play things," says Mr Donnelly. "It's a militarised conception of how to operate."

It has catapulted the GRU into a central role in Russia's engagement with its adversaries. "The GRU has become very significant," says James Sherr, associate fellow at the Chatham House think-tank. "And if you're very significant then in the Russian system you expand."

It is a volatile situation. Real-world tensions between Russia and NATO are running high in militarised zones like the Baltic and the Black Sea. "Cyber space," jokes a recently retired senior British general, "is the new Balkans."

Additional reporting by Max Seddon

How TV5Monde imposed digital detox after attack

For the first six months after APT 28's attack on TV5Monde, the broadcaster went back to a pre-digital era.

There was just one secure computer on each floor. Staff had to queue, rarely less than 20 of them in the line, just to check their emails. Messaging services like Skype were banned. People could not use external flash drives. Uploaded files had to be rigorously decontaminated first.

Yves Bigot, TV5Monde's director-general, has found a new vocation as an evangelist for cyber security. There is still no obvious motive for why the broadcaster was hit. That should be a warning to any large modern company, says Mr Bigot, that anyone, in any industry, is a target. He has few words of comfort. "The digital world is supposed to be fun and easy and cool and natural. But now it's just the opposite," he says.

When the network's staff are abroad, their passwords change every time they log in. Phones cannot be plugged into computers to charge batteries. "What it comes down to basically is, we won't go back to normal ever again, whatever normal is."

Mr Bigot says TV5Monde is lucky. It has learnt and adapted. Other businesses will have to do so too.

"Other companies I speak to understand they have to do something," he says. "But it's like when you're driving. The accident is never going to be you because you're careful and you're a good driver and you don't drink. Until it has happened to you […] you don't take it seriously."

AP PHOTO

The Kuwait city skyline is seen through the haze of a sandstorm

The new Jaber Hospital

In Kuwait, 'too many foreigners' becomes a frequent refrain

By Hussain Al-Qatari

KUWAIT'S first new government hospital in more than three decades will soon open its doors — but only to Kuwaiti citizens.

It's the latest in a series of steps targeting foreigners, including laborers who build high-rise towers, sweep the roads and clean toilets in this tiny oil-rich emirate: a group that far outnumbers the native population.

The 304 million dinar (USD997 million) Jaber Hospital, about a 20-minute drive from downtown Kuwait City, is expected to open in the coming months. It will be the first government hospital built in Kuwait since 1984, taking some pressure off an overburdened public health system.

U.S. ally Kuwait, like other oil-rich Persian Gulf states, has for decades offered a free cradle-to-grave health care for its citizens, along with plenty of generous perks such as subsidized utility prices and housing grants.

But services have been fraying in recent years — despite the cushion of several hundred billion dollars that Kuwait has been building since the 1970s, mostly in a fund for future generations. That money, which stays out of the state budget, is meant to provide for Kuwaitis when the oil runs out. It carried Kuwait through the expenses of the seven-month Iraqi occupation and the 1991 U.S.-led Gulf War that liberated it.

Expatriates with residency and work visas in Kuwait get subsidized health care. A foreign laborer — usually from another Arab country or an Asian migrant — would pay 1 Kuwaiti dinar ($3.2) to see a doctor at a public hospital. His employer would typically pay for him an annual health insurance to the government of 50 dinars, or about $160.

Western expats who live and work in Kuwait tend to go to private hospitals as part of lucrative health care packages provided by their employers.

Many see the new, citizens-only hospital as a step too far. "They were granted their workers' visa. They deserve to be treated with dignity," Dr. Yousef al-Muhanna, a 34-year old general surgeon, said of the migrant workers.

The discrimination goes against the Hippocratic Oath, he says. "We are not supposed to look at their passports - we are supposed to deal with their medical conditions."

The shift started sometime last year, when hospitals and clinics in Jahra, west of the capital, and the Amiri Hospital in Kuwait City began barring expatriates from morning visits for non-emergency services.

Recently, lawmaker Safaa al-Hashem told the media in Kuwait's parliament that "expats are crowding our hospitals and competing with us for the air we breathe in hospital waiting rooms."

She complained that many foreigners bring families on visitor visas to enjoy Kuwait's health care benefits, including deliveries, gastric bypass surgeries, cancer treatment, and other procedures.

"Isn't time for us to put an end to this? We must reform the current system; we must impose taxes on expatriates, not on Kuwaitis," she said.

It's not just the health care.

Kuwait's government and politicians have grown more wary of foreigners in other sectors as well in recent years, adopting or promoting a series of policies that target the roughly 3 million expats living and working here.

> "Expats are crowding our hospitals and competing with us for the air we breathe in hospital waiting rooms.
>
> SAFAA AL-HASHEM
> LAWMAKER

Legislation last April increased the price of electricity and water in all residential buildings, but exempted Kuwaiti nationals.

Social media posts and tweets by Kuwaitis and even statements from officials blaming expats for everything — from traffic congestion to the raiding of open buffets by wedding crashers — are becoming all too common.

Earlier this month, when Egypt beat Burkina Faso in the first semifinals match of the soccer African Cup of Nations, Kuwait's ministry of interior warned Egyptian expats — one of the largest Arab communities here — against celebrating their team's win with car parades. The traditional parades are a raucous event, with soccer fans driving around honking their cars, music blasting and flags waving from car windows.

The ministry said it would immediately deport anyone who takes part in "illegal parades" — so the Egyptians kept their partying off the streets.

"As an Arab expat, when you go to the West, they call you a terrorist or refugee," said Egyptian architect Waleed Shalaan, who has been living in Kuwait since 1999 and considers it his home. "You go to the Gulf states, they call you a leech or a parasite."

Recent law changes require foreigners to have a minimum monthly salary of 400 Kuwaiti dinars ($1,309), and spend two years in Kuwait before applying for a local driving license — with the exception of some professions such as doctors, journalists, university professors, and engineers. Housewives and students may not drive, and anyone caught driving without a license can be deported.

Only tourists and others on a visitor's visa can drive with an international license.

After al-Hashem's "air we breathe" comment, fellow lawmaker Abdulkareem al-Kandari called for a special session of parliament to discuss what he called the "alarming increase in the number of expats versus Kuwaiti nationals."

"We refuse to be a minority in our own country," he said — though Kuwaiti nationals already are, with foreigners making up about 70 percent of the population of 4.2 million.

Several lawmakers demanded the government deport 100,000 expats annually to balance the country's demographics.

Without offering details, Hind al-Sabeeh, the minister of social affairs, promised a plan to "balance the demographics of the country over the next five years, without disrupting the balance of work."

Hind Francis, an analyst at the Rai Institute think tank, said xenophobic sentiments have been on the rise in Kuwait as a way to deflect blame from the authorities.

"Many big problems that concern the public are blamed on the expatriates: congested roads, overcrowded hospitals, many areas in which public policy has failed," she said.

Sarah al-Qabandi, a 35-year old corporate social responsibility manager in the private Ooredoo Telecom says that blaming Kuwait's problems on the expats is a shame.

"We expect people abroad to treat us like royalty [...] we want to be treated well, and yet we don't welcome anyone in our own country," she said. **AP**

Singapore plans Southeast Asia's first carbon tax from 2019

BLOOMBERG

By Dan Murtaugh

SINGAPORE plans to implement Southeast Asia's first carbon tax starting in 2019, a move that would raise energy costs in the island nation and require more than 30 big polluters such as power plants to pay the levy.

The proposal would charge between SGD10 (USD7) and SGD20 a ton on emissions of carbon dioxide and five other greenhouse gases, Finance Minister Heng Swee Keat said in a speech outlining the government's 2017 budget. The tax is equivalent to a USD3.50-to-$-7-a-barrel increase in the cost of oil for combustion. It would raise electricity costs by 2 percent to 4 percent, according to a government report released after Heng's speech.

"The most economically efficient and fair way to reduce greenhouse gas emissions is to set a carbon tax, so that emitters will take the necessary actions," Heng said. "Singapore is vulnerable to rises in sea level due to climate change. Together with the international community, we have to play our part to protect our living environment."

The revenue from the tax would help fund industry measures to reduce emissions, Heng said. The government has been consulting with industry leaders and plans to begin public meetings on the tax in March before deciding on a final tax and implementation schedule. The government also hopes the move will spur job creation in clean energy.

Singapore would be the first Southeast Asian nation to put a price on carbon. Japan has a national carbon tax along with some regional emissions trading markets, and South Korea and New Zealand have national emissions trading. China has several regional trading markets and is planning to launch the world's largest national carbon market this year.

"Singapore looks to be taking a more aggressive course of action on reducing its greenhouse gas footprint than it agreed at the Paris climate talks," Chris Graham, Wood Mackenzie Ltd.'s vice president for energy research, said by phone from Singapore. "These signal concrete plans to put a price on cleaner air."

The biggest impacts would be felt on power generators and heavy industrial users, such as oil refineries, he said. Singapore uses natural gas, the cleanest burning fossil fuel, for the vast majority of its power generation. The tax may spur some investment in renewable energy, although Singapore doesn't have much land for such developments, and increased energy efficiency by end-users, Graham said.

The government will have to work with industrial users to make sure the tax doesn't raise the cost of business to a level that makes them unable to compete with similar firms in the region that don't have to pay for emissions, Graham said.

The tax will be applied on direct emissions of petroleum burned in refineries, but not on the crude oil being processed into gasoline and diesel and other fuels, Singapore's National Climate Change Secretariat said in a statement.

Royal Dutch Shell Plc, which operates one of three oil refineries in Singapore, said it supported in general government-led efforts to price carbon emissions, and would evaluate this particular proposal's impact on its operations as more details emerge.

> **Singapore looks to be taking a more aggressive course of action on reducing its greenhouse gas footprint than it agreed at the Paris climate talks.**
>
> CHRIS GRAHAM

"We would emphasize the critical importance of a policy design which addresses strong economic growth and the competitiveness of Singapore companies in the international market place," a Shell Singapore spokeswoman said in an e-mailed statement. "It must ensure companies can compete effectively with others in the region who are not subject to the same levels of CO2 costs."

Exxon Mobil Corp., which operates another oil refinery in Singapore, said it's committed to working with the Singapore government to balance the risks of greenhouse gas emissions with the need to maintain a strong economy. "A uniform price of carbon applied consistently across the economy is a sensible approach to emissions reduction," spokesman Aaron Stryk said in an e-mailed statement. **Bloomberg**

ASK THE VET

by Dr Ruan Du Toit Bester

5 Common Problems With Dog Toenails

Dog toenails, while seemingly tough, can have problems that if left untreated, can cause a significant amount of pain to the dog. Most frequently many of these problems can be avoided by simply keeping the dog's nails trimmed to an appropriate length.

- Overgrown nails are the most common nail problems for dogs. Most dogs in Macau don't get the activity it takes to keep their nails worn to a good length. The nails should be regularly trimmed to maintain good condition. Overgrown nails can break, split or tear, potentially causing pain and providing an inroad for infection.
- Cracked toenails, if not caused by being overgrown, can often be a sign of an improper diet or possibly an immune deficiency.
- Torn nails can be one of the most painful toenail problems for a dog. A nail may snag on carpeting, a sweater or fabric and tear when the dog tries to get free. This often leads to the nail tearing into the quick, causing bleeding and pain.
- Fungal infections will typically occur if the dog's immune system is depressed either by disease or certain medications. Inflammation in the foot may make the foot tender, causing the dog to limp.
- Bacterial infections are most often a problem brought on by the dog's body trying to fight another disease. The foot/toes will be warm and painful, causing the dog to limp.
- Good dog nail care and proper nutrition can help dogs avoid toenail problems by keeping the nails short and the immune system strong.

Hope this helps
Till next week
Dr Ruan

Ask the Vet:
Royal Veterinary Centre
Tel: +853 28501099, +853 28523678
Emergency: +853 62662268
Email: royalveterinary@gmail.com